Risk Management Strategy

Table of Contents

Introduction 5
Purpose 5
Scope 5
Definitions 6
Why Risk Management is Important 6
Risk Management Objectives 6
Context 6
Ownership 7
Roles and Responsibilities 7
- Council 8
- Audit and Risk Committee 8
- Chief Executive Officer 8
- Executive Leadership Team 9
- Governance and Risk Officer 9
- Managers 9
- Risk Owners 10
- Risk Treatment Owners 10
- All Staff 10
- Contractors 10

Enterprise Risk Management 11
Risk Management Principles 11
Risk Management Framework 12
- Major Elements 13
- Senior Management Support 15
- Integration with Strategic and Business Planning 16

Risk Management Process 16
- Communication and Consultation 17
  - Internal Communication and Consultation 17
  - External Communication and Consultation 17
  - Communication and Consultation Planning 17
- Establishing the Context 18
  - Risk Impact Categories 18
  - Risk Appetite 19
  - Authority for Acceptance of Risk above Tolerance Levels 19
- Risk Identification 20
  - Common Risk Description Structure 21
- Risk Analysis 21
  - Likelihood 22
  - Consequence 23

Determining the Overall Risk Level/Score 23
Controls 24
Risk Evaluation 25
Risk Treatment 25
Treatment Options 25
Cost Effectiveness of Risk Treatments 27
Residual Risk 27
Risk Escalation 28
Contingency Plans 28
Monitoring, Reporting and Review 28
Risk Review and Reporting Frequency 28
Measurement of Performance 29
Compliance 29
Maturity 30
Value Add 30
Retiring Risks 31
Resourcing 32
Documentation 33
Conclusion 33
Appendices 34

Index of Figures

Figure 1: Risk Management Accountability and Reporting Levels 7
Figure 2: Inter-relationship of the Risk Management Principles, Framework and Process 11
Figure 3: Relationship of the Components of the Risk Management Framework 13
Figure 4: Elements of the Risk Management Framework 16
Figure 5: Risk Management Process 16

Index of Tables

Table 1: Risk Impact Categories 18
Table 2: Risk Appetite Rating 19
Table 3: Authority for Acceptance of Risk above Tolerance Levels 20
Table 4: Risk Description Structure 21
Table 5: Example Risk in Risk Description Structure 21
Table 6: Likelihood Rating Matrix 22
Table 7: Consequence Rating Matrix 23
Table 8: Risk Scoring Matrix 23
Table 9: Calculating Risk Level against Risk Categories 24
Table 10: Effectiveness of Control Measures 25

Table 11: Risk Acceptance Criteria 27
Table 12: Risk Reporting Requirements 28
Table 13: Residual Risk Levels and Review Frequency 29
Table 14: Risk Management Maturity Scale 30
Table 15: Example Value Add Key Performance Indicators 30
Table 16: Approval for Retirement of Risks 31
Table 17: Resourcing Strategy 32

Introduction

The City of Kwinana envisions *"A unique and liveable City, celebrated for its diverse community, natural beauty, and economic opportunities"*. As part of this vision, the City aims to embed risk awareness and ongoing monitoring and management at both strategic and operational levels.

This Risk Management Strategy (Strategy) outlines the City's approach to risk, it underscores the City's commitment to enhancing its capability to identify and manage risks as part of its business practices.

Purpose

Regulation 17 of the *Local Government (Audit) Regulations 1996* requires the Chief Executive Officer (CEO) to review the appropriateness and effectiveness of the City's systems and procedures in relation to risk management, internal control and legislative compliance. The review may relate to any or all these three matters, however each of these matters is to be the subject of a review not less than once every three financial years.

This Risk Management Strategy has been developed to support the requirements of Regulation 17, it outlines the City's approach to risk, aligned to AS ISO 31000:2018 Risk Management - Guidelines.

The Strategy confirms the Council's commitment to improving its capability to identify and manage risks as an integral part of business practices.

In implementing the Risk Management Strategy, it is important to ensure:

- Risk management practices support Council's Strategic Community Plan and Corporate Business Plan;
- A consistent and coordinated City wide approach to risk management;
- A risk aware workforce and an environment that supports informed and responsible risk behaviours to protect the community, employees and contractors;
- City risk areas are identified, significant risks are assessed and appropriate controls and treatments are put in place to minimise adverse impacts and ensure opportunities can be realised;
- Governance and compliance requirements for risk management are met; and
- Accountability through informed risk decision making and resourcing.

Scope

The City Risk Management Strategy applies to all areas within the City's planning and organisational structure, operations and facilities.

Definitions

Definitions for terms used in this Risk Management Strategy are provided in the glossary at Appendix A.

Why Risk Management is Important

AS ISO 31000:2018 Risk Management - Guidelines describes risk as *"the effect of uncertainty on objectives."* These 'effects' can be positive, negative or both.

While it is not feasible to eliminate all risks, it is possible to manage uncertainty and create an environment where the occurrence of unexpected events is minimised.

Effective management of risks creates value for a local government and its community and contributes to the demonstrable achievement of objectives whether in strategic or project based initiatives or in normal operations.

Risk Management Objectives

The following risk management objectives have been identified for the City:

- Minimise the occurrence of serious injury or loss of life;
- Protect assets and resources, including natural and cultural;
- Meet legislative and compliance requirements;
- Minimise legal liability;
- Minimise disruption to operations and services;
- Minimise financial loss, including through theft or fraud;
- Improve the City's governance, management capability and accountability;
- Ensure an effective response to critical incidents effecting services and operations;
- Effective emergency response and event recovery; and
- Minimise potential damage to reputation.

Achievement of these objectives will require proactive identification and mitigation of strategic and operational risks, rather than a reactive or incidence response approach.

Proactive risk management adds value to the planning process and business activities of the City and increases the probability of achieving the Council's objectives within its available budget.

Context

Risk management is part of the City's strategic and business planning processes and influences the development of strategies and actions. This in turn impacts budgeting and resource allocation decisions.

The Strategy is linked to the City's Business Continuity Plans as well as the City of Kwinana I.T. Disaster Recovery Plan.

Risk management is supported by the Council and driven by the Executive Leadership Team. There is an expectation that all stakeholders will actively participate to ensure that the City's risk objectives are met.

This strategy applies to all areas within the City's planning, organisational structure, operations, and facilities.

Internal Context

The following are important factors influencing the risk management approach within the City:

- Risk management needs to be a dynamic and proactive activity; and

- There needs to be focus on roles, responsibilities and accountability for managing risk.

External Context

The following are important factors in the external environment that influence the risk management approach within the City:

- Legislative and regulatory obligations, including under the *Local Government (Audit) Regulations 1996*, requires the proactive management of risk by the organisation; and
- Successful risk management involves actively working with the community and external stakeholder organisations.

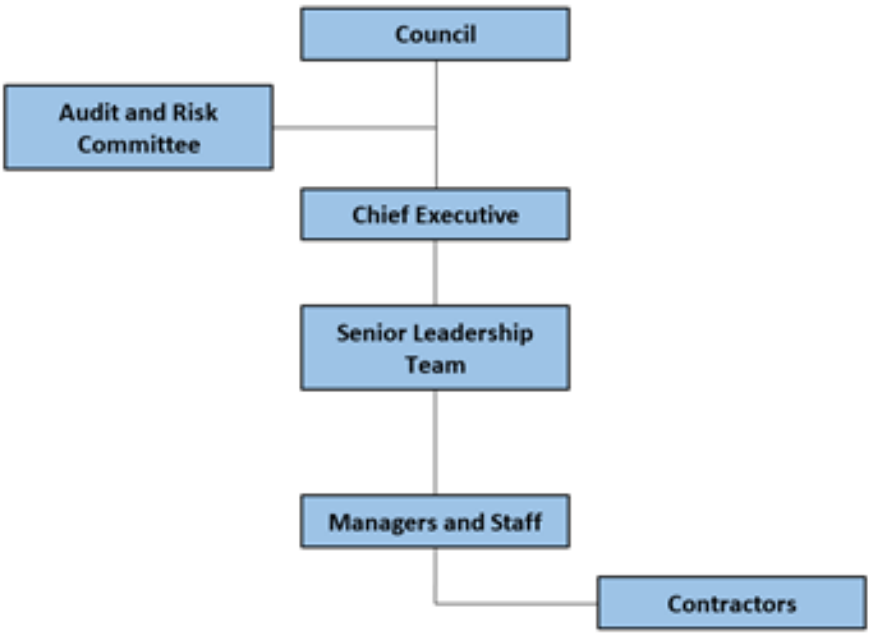
Ownership

The Risk Management strategy is owned by the City's Audit and Risk Committee.

Roles and Responsibilities

Roles, responsibilities, accountability and authority for risk management at the City are summarised in the following chart.

Figure 1: Risk Management Accountability and Reporting Levels



Council

Council has a governance role over the risk management systems of the City, providing both direction and control. The key roles and responsibilities of Council are:

- Ensuring an appropriate risk governance structure is in place;
- Supporting the Risk Management Strategy including risk management as a key element of Councils' strategies, plans and documents; and
- Responsible for setting City's Risk Appetite.

Audit and Risk Committee

The Audit and Risk Committee should support the overall risk management process by:

- Ensuring the City has appropriate risk management and internal controls in place;
- Approving and reviewing risk management programmes and risk treatment options for extreme risks;
- provide guidance and support to management with reviewing risk management tolerances/appetite and making recommendations to Council;
- Providing guidance and governance to support significant and/or high profile elements of the risk management spectrum;
- Monitoring strategic risk management and the adequacy of internal controls established to manage the identified risks;
- Monitoring the City's internal control environment and reviewing the adequacy of policies, practices and procedures;
- Assessing the adequacy of risk reporting;
- Monitoring the internal risk audit function, including development of audit programs as well as monitoring of audit outcomes and the implementation of recommendations;
- note and provide comment on theannual internal audit plan in conjunction with the internal auditor (taking into account the Strategic and Operational Risk Registers) prior to adoption of Council;
- bi-annual review of the organisation's Risk Management Policy and Strategy via the Audit and Risk Committee meeting and provide comments and recommendations to Council.

Chief Executive Officer

The key roles and responsibilities for risk management at the City for the Chief Executive Officer ('CEO') are listed below. In carrying these out, the CEO is assisted by the Audit and Risk Committee and Council.

- Reporting extreme and high risks to the Audit and Risk Committee and/or Council with treatment actions;
- Oversight of the risk management process;
- Promotion of a risk aware culture within Council through the risk management programme;
- Providing direction and advice on the management of risks within Council and ensuring that appropriate treatment measures are in place to mitigate Council exposure;
- Promoting a culture of risk management and ensuring strategic, comprehensive and systematic risk management programmes operate throughout Council;
- Ensuring that the Council's organisation vision and values (relevant to risk) are aligned and synchronised with the strategic direction (including community outcomes and budgetary considerations) and culture;
- Ensuring that risk management is considered in everything Council undertakes and is incorporated in the messages given to the organisation;
- Supporting the Audit and Risk Committee in performance of its duties; and
- Supporting the internal audit process.

Executive Leadership Team

The key roles and responsibilities for the Executive Leadership Team are listed below.

- Maintaining the overall responsibility for the effective and efficient management of all types of risks related to City activities and delivery of the Risk Management Strategy and objectives;
- Promotion of a risk management culture;
- Communicating and raising awareness of risk management to City managers and staff;
- Identifying, managing, and monitoring risks in their areas of responsibility;
- Assisting in setting the Council's risk attitude;
- Ensuring that Council's assets and operations, together with liability risks and hazards to the public, are adequately protected through appropriate risk planning and budgeting, internal audit processes, and appropriate internal systems and controls;
- Ensuring that risk management is in place and reviewed as required and at least annually for all risks for timely updating and continuous improvement;
- Ensuring legislative and governance requirements and obligations are met; and
- Integrating risk management with Council's policies, process and practices.

Governance and Risk Officer

The key roles and responsibilities of the Governance and Risk Officer are listed below.

- Coordinating the risk management process;
- Monitoring the risk profile, risk appetite and effectiveness of controls;
- Monitoring and reviewing high and extreme risks and the implementation of risk treatment plans/actions, as well as to assess compliance and effectiveness;
- Reporting extreme and high risks to the Executive Leadership Team along with treatment plans;
- Facilitating the management of cross-organisational risks;
- Reviewing how the Risk Management Policy and Strategy is communicated throughout the organisation to ensure it is embedded as part of the City's culture;
- Assisting with the development and maintenance of the strategic and operational risk registers;
- Measuring and reporting the effectiveness and adequacy of risk management and internal control processes and systems, and report to the Executive Leadership Team, Audit and Risk Committee and Council;
- Assisting with the education of staff in risk management; and
- Retaining independent risk management consulting expertise to advise the Audit and Risk Committee and assist in the conduct of risk related issues.

Managers

The key roles and responsibilities of Managers are listed below.

- Responsibility for the registration and maintenance of risks in the risk register pertaining to their areas of responsibility as well as at a City-wide operational level as required and appropriate;
- Managing of activities, projects and asset risks as required and appropriate;
- On-going identification and assessment of risk and appropriate responses;
- Management of the relevant risks as delegated within the agreed acceptable risk tolerance levels;
- Ensuring the effectiveness of risk controls;
- Responsibility for ensuring risk management and processes are imbedded in strategies, policies, business plans, contracts, and standard operating procedures; and
- Proactive in implementing best practice in all facets of business including asset management planning, emergency management planning, and disaster and recovery plans.

Risk Owners

The Risk Owner is assigned responsibility for the management of risks, based on their role within the respective area and their ability to competently analyse and treat risks. The key roles and responsibilities of Risk Owners are listed below.

- Ensuring that the risks assigned to them are managed in accordance with the Risk Management Strategy;
- Ensuring that risk treatment actions are completed on time and within budget;
- Reporting to Senior Management on risk treatment action progress in a timely manner;
- Escalating risks to the appropriate level if risk treatments or actions fall outside the delegation of the original risk;
- Escalating to the appropriate level if there are unresolved disputes in relation to shared risks (i.e. risks that apply across organisational areas/functions or involve external stakeholders); and
- Seeking approval to exceed the prescribed level of risk or Risk Appetite and continue to tolerate or retain a higher level of residual risk.

Risk Treatment Owners

A Risk Treatment Owner is assigned the responsibility for the management of risk treatment(s).

The key roles and responsibilities of Risk Treatment Owners are listed below.

- Managing the implementation of specific risk treatment actions; and
- Providing risk treatment implementation progress reports to Risk Owners.

All Staff

All staff will:

- Have an awareness of the risk management framework; and
- Identify, monitor and report issues and potential risks as they occur.

Contractors

The role and responsibilities of contractors are listed below.

- Ensuring the City’s assets and operations, are adequately protected through adherence to Council’s policies and procedures;
- Ensuring liability risks and hazards to the public are appropriately managed in accordance with the risk management framework and in a manner that will not expose the City to loss or risk;
- Responding immediately to the investigation of any report of a hazard or incident received from a resident, City officer, employee or visitor;
- Adhering to legislative, regulatory and corporate legislation and standards; and
- Maintaining appropriate and adequate insurances as required under their contract;

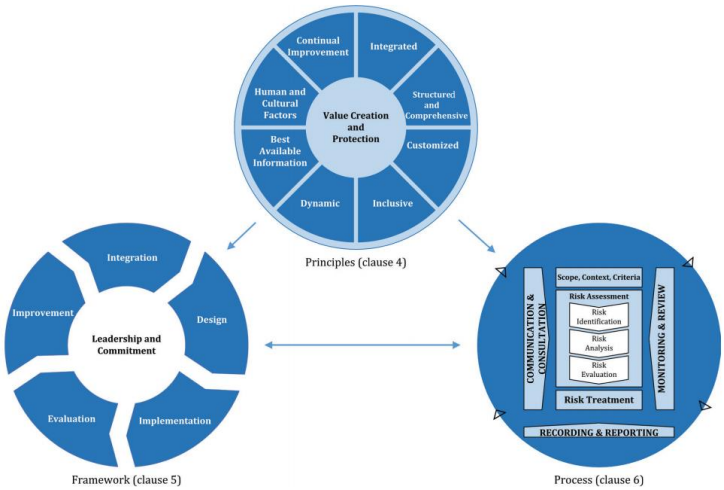
Enterprise Risk Management

The City has adopted an Enterprise Risk Management (ERM) model that is aligned to the *Risk Standard, AS ISO 31000:2018*. The model is comprised of three key components:

1. **Principles for Managing Risk –** the Standard establishes a number of principles that need to be satisfied before risk management will be effective.
2. **Framework for Managing Risk –** the Standard recommends that organisations should have a framework that integrates the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture.
3. **Process for Managing Risks –** an effective process that can be applied across all areas and levels of an organisation, as well to specific functions, projects and activities.

The inter-relationship between the three components is illustrated in the diagram below.

Figure 2: Inter-relationship of the Risk Management Principles, Framework and Process



(AS ISO 3100:2018)

Risk Management Principles

The Risk Management Principles outlined in the *AS ISO 31000:20018 Risk Management - Guidelines*, are essential to developing a "risk culture" to support a successful Enterprise Risk Management model at the City.

An effective risk culture informs decision making by the Executive Leadership Team, management and staff across the City. It builds an understanding that risk management applies to everyone as they aim to achieve City's business objectives.

The City adopts the following Risk Management Principles at all levels of the organisation:

- **Integrated**
  Risk Management is an integral part of all organisation activities.
- **Structured and comprehensive**
  A structure and comprehensive approach to risk management contributes to consistent and comparable results.
- **Customized**
  The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
- **Inclusive**
  Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
- **Dynamic**
  Risk can emerge, change or disappear as an organization's external and internal content changes. Risk Management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
- **Best available information**
  The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
- **Human and Cultural Factors**
  Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
- **Continual Improvement**
  Risk Management is continually improved through learning and development.

Risk Management Framework

The *AS ISO 31000:2018 Risk Management - Guidelines*, defines a Risk Management Framework as a "set of components that provide the foundations and organisational arrangements for integrating, designing, implementing, evaluation, improving risk management throughout the organisation".

Through the City's Risk Management Policy, Strategy, and demonstrated Executive Leadership Team commitment, the Risk Management Framework supports risk management practice, reporting, responsibilities and accountabilities at all levels.

The success of the Risk Management Framework also depends on the effectiveness of the processes that embed it throughout the City.

The Framework provides a conceptual structure for communicating risk information, promoting greater awareness and co-ordination of risk management processes. It also identifies how risk management will be monitored and reported.

The following diagram shows the relationship between the components of the Risk Management Framework.

Figure 3: Relationship of the Components of the Risk Management Framework

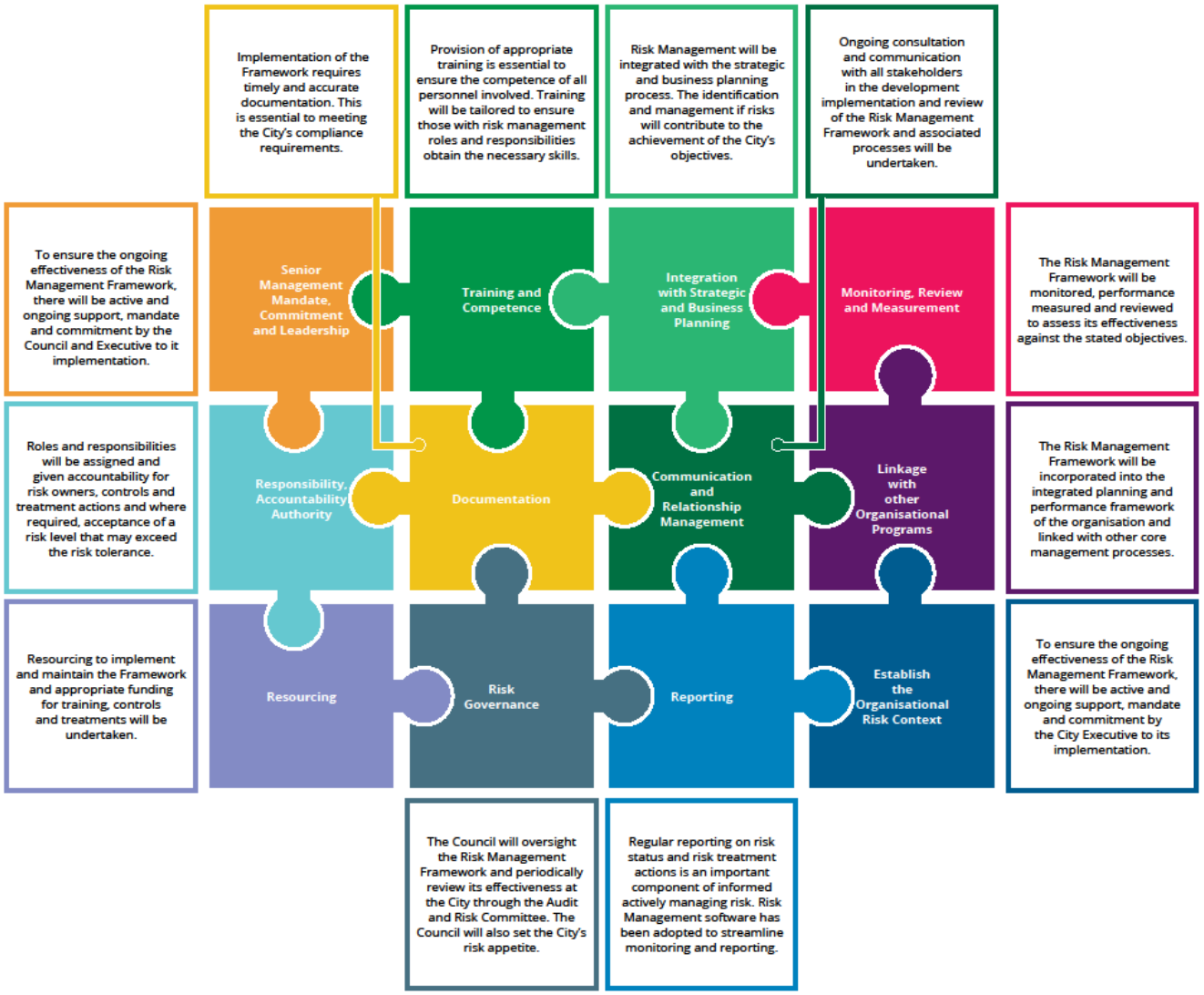
Figure 3 — Framework

Major Elements

The major elements of an effective Risk Management Framework are shown in figure 3, together with a description on how each of these will be applied by the City.

Figure 4: Elements of the Risk Management Framework

Figure 5: Elements of the Risk Management Framework



Senior Management Support

To ensure the ongoing effectiveness of the Risk Management Framework, it is critical that there is active and ongoing support by the City's Executive Leadership Team.

It is important to develop and maintain a risk management culture and awareness of risk and of the impacts of exposure to risk. It is also vital that all levels of management in the City provide unqualified support for the Framework and are actively demonstrating and communicating that support.

Demonstrating Support

Executive Leadership Team support will be demonstrated by:

- Leadership through involvement in the risk management process;
- Membership of the appropriate Committees reviewing risk;
- Prioritising and allocating resources based on risk;
- Championing of stakeholder relationships;
- Effective escalation of risks (where appropriate) and continual follow up;
- Acceptance of accountability for risks outside the tolerance and authority;
- Acknowledging, rewarding and publicising effective risk management;
- Asking the right questions of staff and contractors. The questions should not be limited to how many risks the area currently has. Managers and senior managers alike should be asking:
    - Do I understand the risk?
    - Is the risk description clear and formatted correctly?
    - Is the risk appropriate and relevant to the area?
    - Has the risk been accepted for retention and approved?
    - Is the risk level justifiable based on the assumptions?
    - Are the treatment actions appropriate and cost effective?
    - What is the assessed current level of risk (i.e. how close is the risk to the target level of residual risk)?
    - Have the treatment actions been adequately resourced, budgeted and scheduled?
    - Are the 'downstream' consequences of the treatments understood?
    - Have completed treatment actions been recorded in the risk register?
    - Can the residual risk score (i.e. post-mitigation risk level) be supported based on the effectiveness of the actions?
    - If the residual risk score is still above the level of authority of the manager, has the risk been appropriately escalated?
    - Are risk reviews being conducted and are the results of these reviews documented in the risk register?

By being more involved in the review of risks, the Executive Leadership Team can be assured that the outputs of the Risk Management Framework will have the desired result of reducing uncertainty and increasing the probability that outcomes at all levels will be achieved.

Integration with Strategic and Business Planning

The identification and assessment of risks is an integral part of strategic and business planning processes.

In strategic and business planning risks will be identified, assessed and where appropriate, additional treatments to existing controls identified to minimise the likelihood of the risk event occurring and/or the severity of the consequences.

For strategic planning the following type of risks will be considered:

- Strategic risks; and
- Strategy implementation risks (could be strategic or operational risks).

For business planning the following type of risks will be considered:

- Operational risks; and
- Project risks (for major capital projects).

Failure to incorporate risk management in the integrated planning process significantly reduces its effectiveness.

Risk Management Process

The Risk Management process to be followed within City is shown in Figure below and is in accordance with the *AS ISO 31000:2018 Risk Management –Guidelines*.

Figure 6: Risk Management Process

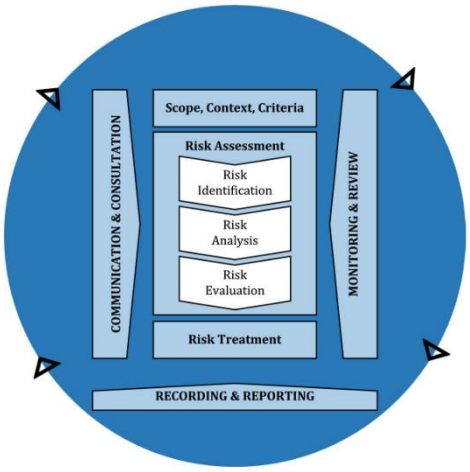


Figure 4 — Process

This process provides a structured approach to managing the City's Risks.

Each of the Risk Management Process steps is described in more detail in the following sections.

Communication and Consultation

Communication and consultation with internal and external stakeholders needs to take place at all stages of the risk management process. This will ensure that those responsible and accountable for implementing risk management understand the basis on which decisions are made and why particular actions are required.

Implementation of the Strategy involves the development and review of plans, programs and services which involves ongoing consultation and communication with stakeholders (both internal and external). These stakeholders should include all those who may be involved in or affected by the City's risk management decisions and actions.

Consultation and proactive stakeholder engagement can assist in clarifying the link between statistical evidence and the perception of risk.

Effective communication and consultation with the City's stakeholders aims to:

- Bring different areas of expertise together for each step of risk management processes;
- Ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;
- Provide sufficient information to facilitate risk oversight and decision making;
- Build a sense of inclusiveness and ownership among those affected by risk.

Internal Communication and Consultation

Communication and consultation within the City builds a risk aware workforce and supports accountability and ownership of risk.

This includes the following:

- Key components of the Risk Management Strategy and Framework and any subsequent modifications;
- Relevant information derived from the application of risk management is available to staff at all levels of the organisation;
- Processes are in place for consultation to occur with internal stakeholders; and
- provision of a risk management software system to support the implementation and maintenance of the City's Risk Management Framework.

External Communication and Consultation

Communication and consultation with the City's external stakeholders supports effective engagement, exchange of information and helps build confidence in the organisation.

This includes the following:

- External reporting to meet legislative/regulatory and governance compliance requirements;
- Communication with stakeholders in the event of a crisis or contingency; and
- Communication with stakeholders on the City's management of risk.

Communication and Consultation Planning

Because stakeholder communication and consultation needs to take place at each level of the risk management process, planning can ensure that this done in a considered and systematic way.

An effective communication and consultation plan should:

- Identify the stakeholders, both primary and secondary;
- State the communication and consultation objectives;
- Identify the most appropriate methods to be used for each group; and
- Have an evaluation process to determine if objectives are being met.

Establishing the Context

Establishing the context defines the external and internal parameters within which risks will be managed at the City as well as sets the scope and risk criteria for the rest of the risk management process. Although similar to those considered in the design of the Risk Management Framework, the parameters are considered here in more detail and with reference to how they relate to the risk management process.

Risk Impact Categories

The Risk Impact Categories are those areas against which the consequences/impacts of risk will be measured at the City and are described in the table below.

Table 1: Risk Impact Categories

Risk Impact Category	Description
Environmental	Harm to the environment or heritage asset or area.
Financial	Financial loss that may or may not be managed within the existing budget and may or may not impact a service.
Health and Safety	Harm or injury to people with potential time loss and/or medical expenses.
ICT, Infrastructure and Assets	Damage to assets/infrastructure with financial consequences. Loss of utilities/ICT systems resulting in disruption to services.
Legislative Compliance	Breach of legislation and compliance requirements that may or may result in legal action and financial penalties.
Reputation/Image	Media exposure that may or may not impact reputation and image and may or may not require action or intervention.
Service Delivery	Disruption to a service or major project in progress that may result in delays to delivery.

Risk Appetite

The ISO Guide 73:2009, Risk Management – Vocabulary defines risk appetite as “The amount and type of risk that an organisation is willing to pursue or retain”.

The AS ISO 3100:2018 Risk Management – Guidelines defines risk attitude (in the context of risk evaluation) as an “Organisations approach to assess and eventually pursue, retain, take or turn away from risk.

Risk appetite or risk attitude is in practice quite difficult to universally define for an organisation, as it varies between risk categories. For this reason, the risk appetite/attitude for residual risk has been identified for each Impact Category for the City in the following table.

Table 2: Risk Appetite Rating

Impact Category	**Level of residual risk the City is willing to retain**			
	Low	Moderate	High	Extreme
Environmental		●		
Financial	●			
Health and Safety	●			
ICT, Infrastructure and Assets		●		
Legislative Compliance	●			
Reputation/Image		●		
Service Delivery		●		

The moderate rating for Environmental, ICT/Infrastructure/Assets and Service Delivery categories reflects the reality that it is not possible to provide the resources necessary to ensure that the level of residual risk will be low in every instance and to manage the escalation process that would result.

The aim is to apply control measures to minimise residual risks to the prescribed tolerance level or below. Any residual risks above the prescribed tolerance level are to be escalated and assigned to the appropriate level within the City. They can then be actioned/resourced to bring the risk back within the prescribed tolerance level.

Authority for Acceptance of Risk above Tolerance Levels

Approval is required to exceed the prescribed level of risk or Risk Appetite and continue to tolerate or retain a higher level of residual risk.

The assigned authority for control and management (including retention) of residual risk above the prescribed tolerance for City risks is shown in the table below.

Table 3: Authority for Acceptance of Risk above Tolerance Levels

Impact Category	Authority for Continued Tolerance/Retention of City Risks			
	Low	Moderate	High	Extreme
Environmental	Director	Director	Chief Executive	Chief Executive
Financial	Director	Director	Chief Executive	Chief Executive
Health and Safety	Director	Chief Executive	Chief Executive	Chief Executive
ICT, Infrastructure and Assets	Director	Director	Chief Executive	Chief Executive
Legislative Compliance	Director	Chief Executive	Chief Executive	Chief Executive
Reputation/Image	Director	Director	Chief Executive	Chief Executive
Service Delivery	Director	Director	Chief Executive	Chief Executive

From Table 4 it can be seen that risks that are High or Extreme for all Impact Categories are outside the City's Risk Appetite and Risk Tolerance and must be managed to reduce the level of risk exposure. Where the level of risk cannot be reduced, approval must be obtained from the CEO to proceed with treatment options for avoiding, treating, transferring/sharing or accepting the risk.

Where the identified risk/hazard has the potential to cause immediate danger to people, the situation needs to be stabilised before the issue is escalated in accordance with the risk escalation process..

Risk Identification

The aim of risk identification is to generate a list of risks based on the event(s) that might create, enhance, prevent, degrade, accelerate or delay the achievement of the City's objectives. It is important to find the right balance between comprehensively identifying risks and not over-doing the process resulting in an unmanageable number of low impact risks.

Risk identification should include risks whose source is not under control of the City, or is not evident. It should also consider a wide range of consequences and their follow-on effects (including cascade and cumulative effects). All significant causes and consequences need to be considered.

The following questions are important in the risk identification process:

- What might happen or what can go wrong i.e., the risk event?
- What would cause it to happen?
- What would the effect on the Council's objectives be?

To ensure their effectiveness, risk identification should involve members of the wider stakeholder community where appropriate.

Common Risk Description Structure

Identified risks need to be described in a consistent manner so that they can be readily understood by all stakeholders. The common method for describing risks to be used at the City is shown below.

Table 4: Risk Description Structure

Item	Description
Name	Relate name to system impacted and explanation of cause
Cause/s	Explanation of what might cause the risk event to occur (list each cause)
Consequence	Identify local consequences and attempt to identify how these affect major areas

An example of a risk in this format is shown below.

Table 5: Example Risk in Risk Description Structure

Item	Description
Name	Injury from manual handling
Cause/s	Failure to comply with policies and procedures related to manual handling Poor staff training Failure to comply with mandated training Poor equipment maintenance Lack of appropriate equipment Failure to undertake worksite inspections Poor risk assessment of task Poor hazard identification Lack of incident reporting
Consequence	Workplace injury claim and lost days Litigation relating to breach of Work Health & Safety duties Adverse publicity relating to event

Risk Analysis

The aim of risk analysis is to differentiate minor acceptable risks from major risks, and to provide data to assist in the evaluation and treatment of risks.

Risk analysis involves considering the causes and sources of risk, their consequences (effects) as well as the likelihood of such consequences occurring.

Risk level is determined by combining both the estimates/rating of consequence and the likelihood, in the context of the existing control measures.

It is important to recognise that the consequence and likelihood ratings are estimates. As such, they should involve a range of perspectives from the wider stakeholder community.

It is preferable that those conducting the risk analysis have been provided with the appropriate training to facilitate a more objective assessment. Analysis can be quantitative, qualitative or semi-qualitative in nature, depending on the type of risk as well as the availability and quality of data and information.

It is important to determine the most probable/conceivable consequence and likelihood rather than automatically stating the most extreme result. For example, stating that exposure to any hazard could almost certainly result in death would result in the City wide risk profile being unnecessarily skewed to the high to extreme end of impact.

Likelihood

All areas within the City will use the likelihood rating system for analysing risks shown in the table below.

Table 6: Likelihood Rating Matrix

Likelihood Rating	Continuous Time Based (e.g. project duration or financial year)	Annual Return Period	Activity/Frequency Based	Probability
Almost Certain A	80-100% probability that the event will occur in the time period being considered.	Likely to occur at least once in every 1 to 1 ¼ years.	The event is likely to occur almost every time the activity is carried out or the organisation is exposed to the hazard.	Over 0.8 (> 4:5)
Likely B	50-79% probability that the event will occur in the time period being considered.	Likely to occur once every 1 ¼ years to 2 years.	The event is likely to occur more often than not when the activity is carried out or the organisation is exposed to the hazard.	0.5 - 0.79 (1:2 - 8:10)
Possible C	25-49% probability that the event will occur in the time period being considered.	Likely to occur once every 2 years to every 4 years.	The event is likely to occur less often than not when the activity is carried out or the organisation is exposed to the hazard.	0.25 - 0.49 (1:4 to 1:2)
Unlikely D	2-24% probability that the event will occur in the time period being considered.	Likely to occur once every 4 years to every 50 years.	The event is seldom likely to occur when the activity is carried out or the organisation is exposed to the hazard.	0.02 -0.24 (1:50 to 1:4)
Rare E	0-2% probability that the event will occur in the time period being considered.	Not likely to occur more than once in 50 years.	The event is not likely to occur when the activity is carried out or the organisation is exposed to the hazard.	0 - 0.02 (< 1:50)

Consequence

As with likelihood, for risk assessments to be effective there needs to be a structured approach across the City to assessing consequence. Refer to Appendix B for detailed Consequence criteria according to rating.

Table 7: Consequence Rating Matrix

Consequence Rating	Description
Insignificant	Effect is minimal
Minor	Event requires minor levels of resource and input for easy remediation
Moderate	Some objectives affected
Major	Some important objectives affected or cannot be achieved
Severe	Disaster with potential to lead to collapse or having a profound effect

Determining the Overall Risk Level/Score

To determine the overall risk level for a particular risk, the likelihood and consequence scores for the risk can be plotted in a matrix, as shown below.

Table 8: Risk Scoring Matrix

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	Medium	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Low	Medium	High	High	Extreme
Unlikely	Low	Low	Medium	High	Extreme
Remote	Low	Low	Medium	Medium	High

Identified risks are to be assessed against all Risk Categories. Because it is not practical to give a risk multiple ratings, the highest consequence rating against the Risk Category is used. This is illustrated in the table below (for revised risk assessment/with controls).

Table 9: Calculating Risk Level against Risk Categories

Risk Name	Likelihood	Risk Category	Consequence	Risk Level
Injury from manual handling	Possible	Accreditation/Legislative Compliance	Moderate	High
		Asset/Infrastructure	Minimum	
		Consumer/Customer/Community Concern	Minimum	
		Employee/Visitor/Contractor Event	Moderate	
		Environmental/Service Event	Minimum	
		Financial	Moderate	
		Patient/Resident	Minor	
		Reputation/Image	Minor	

The City determines the risk level for inherent risk (i.e. without controls). In risk management, this is sometimes identified as the Potential Exposure ('PE') (i.e. the plausible maximum impact arising from a risk if all current controls fail). The risk is then reassessed (revised risk) with controls factored in.

Controls

Controls are those policies, procedures, plans, processes and systems that have been designed and implemented over time in response to risks/issues that have or may occur. Most risks identified will not be new or unique and there may be some controls already in place to manage them.

Controls typically fit into three distinct types:

1. **Preventative Controls** - aimed at preventing the risk occurring in the first place. They include policies, procedures, plans processes and systems;
2. **Detective Controls** - used to identify when a risk has become an issue/incident. They include audits, stocktakes, reviews, etc; and
3. **Mitigating Controls** - aimed at minimising the consequences that arise from the issue/incident. They include Business Continuity Plans, Disaster Recovery Plans, personal protective equipment, etc.

Following the identification of existing controls, it is necessary to evaluate them for effectiveness. The fact that proven processes are being followed does not necessarily mean that risk is being mitigated. The experience level of the personnel undertaking the processes and the rigour with which the processes are being followed and supervised will also impact upon the control effectiveness.

For each risk identified, the following questions need to be asked:

1. Is there anything in place at the moment that would effectively decrease the likelihood or the impact of this risk? If the answer is yes, then:
2. How effective are the current controls in preventing this risk from occurring or reducing the impact?

There is usually a direct correlation between the effectiveness of an existing control and the likelihood of the risk occurring (i.e. the more effective the control, the less likely the risk is to occur) and/or the impact of the risk (i.e. non effective controls may increase the impact).

The outcome of this evaluation should influence further analysis of the likelihood and potential consequences of the risk.

The table below shows the rating and description for the effectiveness of current controls at the City.

Table 10: Effectiveness of Control Measures

Effectiveness Rating	Description
Effective	Fully effective at all times (i.e. will significantly reduce the likelihood and/or consequence of the risk at all times).
Partially Effective	Partial control most of the time (i.e. will have some effect in terms of reducing the likelihood and/or consequence of the risk)
Ineffective	Not effective at all in mitigating the risk (i.e. will not have any effect in terms of reducing the likelihood and/or consequence of the risk)

Risk Evaluation

The purpose of Risk Evaluation is to determine whether a risk needs further treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk level established during the Risk Analysis process with the Risk Appetite and Evaluation Criteria for the City.

In some cases, the Risk Evaluation can lead to a decision to undertake further Risk Analysis. The Risk Evaluation can also lead to a decision not to treat the risk (i.e. just maintain existing controls).

Risk Treatment

Risk treatment consists of determining what will be done in response to the identified, analysed and evaluated risks, including identifying resource implications for the implementation of the treatment actions.

Risk treatment involves a cyclical process of:

a) Assessing a risk;
b) Deciding whether residual risk levels are tolerable;
c) If not tolerable, generating a new risk treatment; and
d) Assessing the effectiveness of that treatment.

Once implemented, risk treatments may become risk controls.

Treatment Options

Risk treatment decisions are guided by a series of questions:

1. Can the risk be avoided altogether by not undertaking the activity?
2. Can the likelihood of the risk occurring be reduced by strengthening/ensuring the effectiveness of current controls?
3. Can the likelihood of the risk occurring be reduced by adding new controls (i.e. initial treatments)?
4. If the event occurs, can the consequences be reduced through sharing the risk with another party or by a Business Continuity Plan/Disaster Recovery Plan?

Where risk treatment options can impact on risk elsewhere in the City, relevant staff or contractors they should be included in the decision making.

Selecting the most appropriate risk treatment option involves balancing the costs of implementation against the benefits with regard to legal, regulatory and other requirements. Decision making

should also take into account such risks where risk treatment is not justifiable (e.g. severe consequence but rare likelihood).

There are four main treatment options for the mitigation of identified risks at the City. These are listed in more detail below.

1. **Avoid**

   Avoiding a risk/event with detrimental consequences by deciding not to proceed with the activity likely to create the risk, or by disposing of the asset, etc.

2. **Treat**

   Treating risks to reduce the likelihood and/or consequence of the risk.

   Where risk treatments are identified for a given risk, the City risk management software compiles a Risk Treatment Plan for each risk. Each risk treatment action has an owner, start and end date, frequency of progress reporting and revision date.

   All risk treatments identified by the City and incorporated in the Risk Treatment Plan need to be adequately resourced to ensure they can be successfully implemented and completed.

   Upon completion of the risk treatments, the Risk Register is to be updated and the risk reassessed as to whether treatment actions have been successful in reducing the likelihood and/or consequence.

3. **Transfer/Share**

   Risk transfer/share involves transferring part of the risk (i.e. either management of the activity/service or consequences) to another party. Sharing risk does not mean that the responsibility/accountability for the risk has been transferred.

   Examples of transferring or sharing of risk include:

   a) **Contracting and/or Insurance** - the most widely used forms of risk transfer. In practice, it is virtually impossible to transfer all of the risk to a third party (e.g. transferring a risk to a contractor could still see the City's reputation damaged should an adverse event/incident occur).

   b) **Escalation** – occurs when there is a requirement for a higher level of line management within the Council to take action in relation to a risk. When a risk has been escalated, management of the risk has not been transferred as the consequences will still impact on the area concerned.

   However, the treatment of all or part of the risk has been transferred to line management. In the case where a risk has been escalated, line management is to maintain active visibility on the progress of actions and report back to the Executive Leadership Team at regular intervals. Reasons for risk escalation include:

   - The residual risk (after treatment risk level) is outside the Risk Tolerance level;
   - The risk treatment actions are outside the control of the City; or
   - The risk owner has attempted risk treatment actions, but they have not been successful

   The overarching principle in relation to risk transfer/share is that if the City owns all or part of the consequences then it still owns the risk.

4. **Accept**

   Accepting the consequences of the risk occurring.

   Risks are accepted or retained for a number of reasons, including:

   a) Risk treatment is not cost effective;
   b) The risk is at or below the acceptable level for that type of risk;
   c) The risk is outside the control of the Council; or

d) The risk exceeds the acceptable level for that type of risk but nothing more can be done to reduce the risk (if this is the case it needs to be escalated and well documented).

Where a decision to accept a risk is taken, the risk needs to be recorded in the Risk Register along with the reason(s) for the decision not to treat the risk.

Cost Effectiveness of Risk Treatments

Determining whether a risk is cost effective is not as simple as identifying the cost of a consequence versus the cost of a treatment.

A risk that may have no direct financial consequence may still have other major or severe consequences (e.g. reputation). In such cases it may be the right decision to still treat the risk to reduce the consequences against the respective Risk Categories, thereby reducing the risk level to within the Risk Appetite of the City.

For this reason it is critical that risks are assessed against all Risk Categories. If risks are not fully assessed, it is difficult to conduct a full assessment of cost effectiveness.

Residual Risk

Residual risk is the risk level remaining after risk treatment options/actions have been implemented. After determining the risk treatments for each risk, the risk is reassessed to determine the post-mitigation risk level (i.e. the residual risk level).

For risks where the decision is taken to accept the risk, the residual risk level will be the same as the pre-mitigation risk level.

The table below summarises the risk acceptance rating and criteria for each risk level at the City.

Table 11: Risk Acceptance Criteria

Risk Level	Risk Acceptance Rating	Risk Acceptance Criteria	Responsibility
Extreme	Unacceptable	Active Management Risk only acceptable with excellent controls and all treatments explored and implemented where appropriate. Managed at the highest level of authority and subject to continuous monitoring and formal monthly review/reporting.	Chief Executive
High	Urgent Attention Required	Regular Monitoring and Review Risk acceptable with excellent controls, managed by senior management and subject to formal quarterly review/reporting.	Chief Executive
Medium	Monitor	Periodic Monitoring Risk acceptable with adequate controls, managed by specific procedures and subject to formal six monthly review/reporting.	Director
Low	Acceptable	Annual Monitoring Risk acceptable with adequate controls, managed by routine procedures and subject to formal annual review/reporting.	Director

Risk Escalation

The escalation of a risk to a higher level of line management to deal with it or for acceptance of a risk beyond the Council's Risk Appetite and Risk Tolerance.

Not all risks can be treated at the local level, however without a structured and documented escalation process, staff at that level may be put in a position where they feel they have to accept a risk beyond their control, authority or accountability.

The Risk Escalation process for the City is automated via the City's risk management software. .

Contingency Plans

Contingency Plans are developed to deal with a risk if it occurs and becomes an issue. The purpose of developing a Contingency Plan is to determine at an early stage the strategy to recover from such a situation and to minimise the impact.

In essence, developing Contingency Plans enables the City to be proactive in dealing with risk issues prior to them arising.

If a Contingency Plan is developed it needs to be costed and will form part of the consequence rating for the risk (e.g. if the risk eventuates, the cost of a facility closure for a protracted period of time needs to be considered in the Consequences).

As a general rule, Contingency Plans should be developed for risks with a pre-mitigation risk score of high or extreme, regardless of the post-mitigation (residual risk) score.

Monitoring, Reporting and Review

The purpose of risk monitoring, reporting and review at the City is to:

a) Provide an understanding of the strategic and operational risk exposure;
b) Identify the priority risks that require management attention;
c) Inform stakeholders on the City's risk profile and management;
d) Provide managers and staff with the necessary information to make informed risk management decisions;
e) Ensure the Risk Policy and Strategy align to the City's internal and external environments;
f) Risk management objectives are aligned to the objectives of the organisation; and
g) Risk management is contributing to organisational performance.

Risk Review and Reporting Frequency

It should be noted that when there is a significant change to circumstances, all risks should be reviewed and reported on at that time. Examples of the types of changes that would trigger a full review include (but are not limited to):

a) Changes to key personnel (e.g. Senior Manager);
b) Significant changes to policy; or
c) Significant changes to the organisational and/or services structure.

Conducting such reviews will ensure that the Risk Registers remains current.

The table below summarises the risk reporting requirements at the City.

Table 12: Risk Reporting Requirements

Report	Frequency	Audience
Risk Treatment Action Status Report	Monthly	Managers
	Quarterly	Audit and Risk Committee

Incident Report	Monthly	Managers
	Quarterly	Audit and Risk Committee
Strategic Risk Report	Quarterly	Senior Management
		Audit and Risk Committee
Operational Risk Report	Quarterly	Managers
		Audit and Risk Committee
Risk Management Strategy and Framework Audit Report	Bi-Annual	Executive Leadership Team
		Council

Monitoring and Review need to be planned as part of the Risk Management process to ensure that risks are being effectively managed.

As few risks remain static, they need to be regularly reviewed for currency and accuracy. Risk assessment, treatment strategies and the effectiveness of mitigation actions need to be monitored to ensure changing circumstances do not alter priorities or expected outcomes.

Risk Owners are to monitor the currency and status of the risks that have been allocated to them and report on them in accordance with the requirements of this plan.

Risks are to be formally monitored and reviewed/reported on by the Risk Owner in accordance with the table below.

Table 13: Residual Risk Levels and Review Frequency

Risk Level	Review Frequency
Extreme	Monthly
High	Quarterly
Medium	Annually
Low	Annually

Measurement of Performance

Risk management performance at the City will be assessed against the following criteria:

1. **Compliance**: measuring compliance with the City's Risk Management Policy and Strategy directives and objectives;
2. **Maturity**: measuring the maturity of the City's Risk Management Strategy and Framework against industry best practice; and
3. **Value Add:** measuring the extent to which risk management is contributing to the achievement of the City's objectives and outcomes.

Compliance

The Risk Management Framework will be audited annually to ensure that the core directives/requirements and objectives detailed in the following the City documents are being complied with:

- Risk Management Policy; and
- Risk Management Strategy

Maturity

To determine the current risk management maturity or progress of an organisation, a critical evaluation or assessment is undertaken to determine the following:

a) How effectively risk management practices are currently being undertaken;
b) How well risk management practices have been integrated into existing management and operational practices;
c) If the Risk Management Framework requires adjustment; and
d) How the risk maturity of the workforce has improved.

Assessments are typically undertaken annually by an independent assessor. They involve a range of development, application, documentation and review items, with an alignment to AS ISO 31000:2018 and requirement for validation. A typical risk management maturity scale is outlined in the table below.

Table 14: Risk Management Maturity Scale

Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Awareness	**Understanding**	**Initial Application**	**Embedded**	**Mature**
There is a general understanding within the organisation of the benefits of risk management to the organisation, however, at this stage, no active measures have been taken that would constitute the implementation of a Risk Management Framework.	A Risk Management Framework has been designed and implementation has commenced or has been programmed to commence in the near future. There may be some risk management being done within the organisation, however, this is on an ad-hoc basis and is reliant on individuals within the organisation, as opposed to leadership from senior management.	A Risk Management Framework has been implemented in all key functional areas within the organisation; however, there are areas within the organisation that have yet to incorporate sound risk management practices into their processes.	A Risk Management Framework has been implemented in all key functional areas within the organisation, however, not all of the functional areas can be regarded as 'best practice' in relation to their risk management but steps are being taken to continually improve.	A Risk Management Framework has been implemented in all key functional areas within the organisation, and all of the functional areas can be regarded as 'best practice' in relation to their risk management.

(Source: Paladin Risk Management Services, 2014)

Value Add

It is more difficult to measure the contribution of the Risk Management Strategy and Framework to organisational performance than it is to measure compliance and risk management maturity.

Performance measurement will focus on measures that demonstrate how well the organisation is managing its risks as indicators of the performance of the Risk Management Framework. The following table lists exampled key performance indicators that could be used for this purpose.

Table 15: Example Value Add Key Performance Indicators

Performance Area	**Key Performance Indicators**
Risk Treatment Plan	% of off-track risk treatment actions
Risk Reviews	% of risk reviews undertaken as scheduled
Incident Management	Number of safety incidents
Risk Training	% of nominated staff undertaking risk management training

Risk Exposure	% of risks exceeding prescribed level of residual risk with authorisation

Retiring Risks

Risks are to be retired after the chance of something happening has clearly passed. It is important that appropriate approval is provided (and recorded in the Risk Register) when a risk is to be retired.

The following table provides the approval authority for the retirement of risks:

Table 16: Approval for Retirement of Risks

Risk Level	Review Frequency
Extreme	Chief Executive
High	Chief Executive
Medium	Director
Low	Director

Within the City context, very few risks will be retired. Risks are not to be retired simply because no treatment is required or treatments have already been implemented and the risk has reached its target level.

Examples of risks that could be retired include risks associated with projects with defined start and end dates.

Resourcing

The City is committed to ensuring risks are managed and resourced in accordance with the Risk Management Strategy and Framework.

The table below summarises the resourcing strategy for key areas of the Risk Management Strategy and Framework.

Table 17: Resourcing Strategy

Area	Resource Requirements	Budget
Risk Treatment Actions	Internal Resources	Operational and Capital Budgets
Risk Management Training	External and Internal Training Resources	Operational Budget
Risk Management Framework Audit	External Provider	Operational Budget
Risk Management System	External Provider	Operational Budget

Training

To ensure persons at all levels of the organisation can effectively carry out their risk management roles and responsibilities, appropriate risk management training will be provided.

Risk Management training at the City will be tailored for the following target audiences:

Council and Executive Leadership Team

- The risk management roles and responsibilities of the Council and Executive Leadership Team;
- An overview of the risk management process and how risks are identified, analysed, and managed; and
- The types of reports that will be received and how to interpret and analyse the information as a basis for making decisions.

Department Managers

- The risk management roles and responsibilities of Department managers;
- More detailed training on the risk management process and how risks are identified, analysed and managed; and
- The types of reports that will be received and how to interpret and analyse the information as a basis for making decisions.

City Staff (and appropriate Contractors)

- General awareness training in the risk management process and hazard identification as it applies to their operational duties.

Documentation

Risk Management Strategy and Framework documentation provides the following benefits:

a) Evidence that implementation has been conducted properly;
b) A body of knowledge for the organisation to work with;
c) A basis for effective review of decisions and processes;
d) An accountability and audit mechanism;
e) Source of information for effective communication with stakeholders;
f) A basis for monitoring and review; and
g) A basis for accreditation.

The following is a list of the documentation necessary to implement and maintain the Risk Management Framework:

1. The City's Risk Management Policy;
2. The City's Risk Management Strategy;
3. The City's Strategic Risk Register; and
4. The City's Operational Risk Register.

Review requirements are specified in each of these documents.

Risk Registers

A critical element of Risk Management is the recording of risks. Risks that are not recorded are not able to be managed and the risk exposure of the Council is unlikely to be increased.

The most effective means of capturing risk is through the use of Risk Registers.

A Risk Register captures all of the information necessary to ensure the risk can be effectively managed.

An effective Risk Register follows the Risk Management Process as defined in the Standard and allows for the capture of all identified risks, the controls and their effectiveness, the assessed risk level, the treatment strategy and individual treatment actions.

The City utilises Camms.Risk software for maintenance of its Risk Register.

Conclusion

The City Risk Management Strategy and Framework together with the Risk Management Policy provide an enterprise wide, integrated approach to risk management.

The Council and Executive Leadership Team have a commitment to implementing, maintaining, reviewing and reporting on the Risk Management Strategy. There is also a commitment to supporting and encouraging a risk management culture throughout the organisation.

Improving the City's maturity in the risk management processes to realise the benefits that come from effective risk management will take commitment from everyone across the organisation.

OFFICER USE ONLY

Officers may amend this section without council approval.

Responsible Team	Governance and Legal	
Initial Council adoption	Date: August 2020	Ref#: 369
Reviewed/amended	Date: October 2022	Ref#: <CM Ref>
Next Review Date	Date: September 2026	
Policy Document Number	D20/44400[v4]	

Appendices

Appendix A: Glossary of Terms

Term	Definition
Consequences	Outcome of an event affecting objectives (AS ISO 31000:2018).
Contingency	Contingency is an allowance for future increases to estimated costs for project cost elements and is the aggregate of amounts (if any) included in the Project Approval: ▪ to meet the assessed risk of project acquisition cost increases that may arise as a result of underestimates due to inherent cost uncertainties; ▪ to meet the residual project risk after all planned risk mitigation/elimination/treatment measures; and ▪ to meet 'unknown unknowns'.
Control	Measure that is modifying risk (AS ISO 31000:2018).
Exposure	The risk exposure is a qualitative value of the sum of the consequences of an event multiplied by the probability of that event occurring.
Likelihood	Chance of something happening (AS ISO 31000:2018)
Residual Risk	Risk remaining after risk treatment (AS ISO 31000:2018)
Risk	Effect of uncertainty on objectives (AS ISO 31000:2018)
Issue/Incident	An event that has occurred that has taken DSO outside its tolerances/Risk Appetite
Risk Acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk Analysis	A process to comprehend the nature of risk and to determine the level of risk (AS ISO 31000:2018).
Risk Appetite	The amount and type of risk that an organisation is prepared to pursue, retain or take.
Risk Avoidance	An informed decision to withdraw from, or to not become involved in, a risk situation.
Risk Identification	Process of finding, recognising and describing risks (AS ISO 31000:2018)
Risk Management	Coordinated activities to direct and control an organisation with regard to risk (AS ISO 31000:2018).
Risk Management Plan	Scheme within a risk management framework specifying the approach, the management components and resources to be applied to the management of risk Coordinated activities to direct and control an organisation with regard to risk (AS ISO 31000:2018).
Risk Register	A Risk Register provides a repository for recording each risk and its attributes, evaluation and treatments.
Risk Source	Element which alone or in combination has the intrinsic potential to give rise to risk (AS ISO 31000:2018).

Term	Definition
Risk Owner	Person or entity with the accountability and authority to manage a risk (AS ISO 31000:2018).
Risk Retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organization. (AS/NZS 4360:2004)
Risk Tolerance	An organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve objectives.
Risk Transfer	Sharing with another party, the burden of loss or benefit of gain, for a risk (AS/NZS 4360:2004)
Risk Treatment	Process to modify risk (AS ISO 31000:2018).
Risk Treatment Plan	The defined approach to treating an identified risk. The plan should include details of who is responsible for implementation; resources required; budget allocated; timetable for implementation; and method of review.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity. (AS ISO 31000:2018)

Appendix B: Consequence Criteria and Rating

Impact Category	Insignificant	Minor	Moderate	Major	Severe
Environmental	Negligible damage that is contained on-site. AND The damage is fully recoverable with no permanent effect on the environment or the asset, It will take less than 6 months for the resource to fully recover.	Minor damage to the environment or heritage asset or area that is immediately contained on-site. It will take less than 2 years for the resource or asset to fully recover, or it will only require minor repair. OR Disturbance to scarce or sensitive environmental or heritage asset or area.	Moderate damage to the environment or a heritage listed asset or area, which is repairable. The resource or asset will take up to 10 years to recover.	Irreversible and extensive damage is caused to a non-Heritage Listed area or asset but that has heritage values. OR Irreversible and extensive damage is caused to a non-environmentally significant area or asset. OR Significant damage is caused to a Heritage Listed area or asset that involves either extensive remediation or will take more than 10 years to recover. OR Significant damage is caused to an environmentally significant area or asset from which it	Irreversible and extensive damage is caused to a World Heritage Listed Area, a National Heritage Listed Site, a Register of the National Estate Site or a Council Heritage Listed area or asset. OR Irreversible and extensive damage is caused to a Matter of National Environmental Significance under the Act (e.g. endangered species, RAMSAR wetland, marine environment).

Impact Category	Insignificant	Minor	Moderate	Major	Severe
				will take more than 10 years to recover.	
Financial	Minimal financial impact requiring no action or approval within local authority levels. Less than $10,000.	A financial loss that can be managed within existing department budget. $10,000 to less than $100,000.	A financial loss that can be managed within existing organisational budget. $100,000 to less than $1M.	A financial loss resulting in potential reduction in a service. $1M to less than $5M.	A critical financial loss resulting in closure or significant reduction in a service. Greater than $5M.
Health and Safety	Minor injury or ailment that does NOT require medical treatment by a physician or a qualified first aid person.	Injuries or illness requiring medical attention with no long-term effects. OR Exposure of public and staff to a hazard that could cause minor injuries or minor adverse health effects	One or more injuries or illness requiring hospitalisation with some long-term effects. OR Public or staff exposed to a hazard that could cause injuries or moderate adverse health effects	One or more serious casualties or illness with long-term effects. **OR** Public or staff exposed to a hazard that results in major surgery or permanent disablement.	One or more fatalities or life threatening injuries or illness. OR Public or staff exposed to a severe, adverse long-term health impact or life-threatening hazard.
ICT, Assets/Infrastructure	Some damage where repairs are required however facility or infrastructure is still operational. Loss of utilities/systems resulting in minor IT	Short term loss or damage where repairs required to allow the infrastructure to remain operational using existing internal resources.	Short to medium term loss of key assets and infrastructure where repairs required to allow the infrastructure to remain operational.	Widespread, short term to medium term loss of key assets and infrastructure. Where repairs required to allow the infrastructure to remain operational.	Widespread, long term loss of substantial key assets and infrastructure. Where infrastructure requires total rebuild or replacement.

Impact Category	Insignificant	Minor	Moderate	Major	Severe
	disruption to a service for up to 12 hours.	Loss of utilities/systems resulting in minor IT disruption to a service (>12 hours - 24 hours).	Cost outside of budget allocation. Loss of utilities/systems resulting in IT disruption to a department for up to 12 hours.	Cost significant and outside of budget allocation. Loss of utilities/systems resulting in serious IT disruption to several services or more than 1 department for up to 12 hours.	Failure of utilities/systems resulting in the loss of function for several departments (> 12 hours).
Legislative Compliance	Minor technical breach but no damages. No monetary penalty AND/OR Internal query.	Minor technical non-compliances and breaches of regulations or law with potential for minor damages or monetary penalty. AND/OR Special audit by outside agency or enquiry by Ombudsman.	Compliance breach of regulation with investigation or report to authority with prosecution and/or possible fine. AND/OR Non-compliance with Corporate/Council Policy	Major compliance breach with potential exposure to large damages or awards. Prosecution with 50% to maximum penalty imposed. OR Multiple compliance breaches that together result in potential prosecution with 50% to maximum penalty imposed	Serious compliance breach with potential prosecution with maximum penalty imposed. OR Multiple compliance breaches that together result in potential prosecution with maximum penalty imposed
Reputation/Image	Customer complaint. AND/OR Not at fault issue, settled quickly with no impact.	Non-headline community media exposure. Clear fault. Settled quickly by the City response. Negligible impact.	Negative local (headline) and some regional media coverage. Council notification. Slow resolution.	Negative regional (headline) and some national media coverage. Repeated exposure. Council involvement. At fault or unresolved	Maximum multiple high-level exposure. Sustained national media coverage. Direct Council intervention. Loss of credibility and public

Impact Category	Insignificant	Minor	Moderate	Major	Severe
				complexities impacting public or key groups.	/ key stakeholder support.
Service Delivery	Some non-essential tasks will not be able to be achieved. AND/OR Unable to provide service for <1 business day. AND/OR Major Project in progress delay for < 1 month.	Less than 5% of essential tasks will not be achieved. AND/OR Unable to provide service for 1-3 business days. AND/OR Major Project in progress delay for 1 - 2 months.	5% - 10% of essential tasks will not be achieved AND/OR Unable to provide service for 3-10 business days. AND/OR Major Project in progress delay for 2-3 months.	10% - 20% of essential tasks will not be achieved. AND/OR Unable to provide service for 10-20 business days. AND/OR Major Project in progress delay for 3-6 months.	Greater than 20% of essential tasks will not be achieved. AND/OR Unable to provide service for >20 business days. AND/OR Major Project in progress delay for > 6 months.