

# Risk Management Policy

## City Policy

### Responsible Directorate: Office of the CEO

**Objective:** The objective of this policy is to communicate the City's commitment and approach to managing risks that may impact on its day-to-day operations and threaten the achievement of its objectives. The risk management process, associated guidelines, policies and monitoring and review processes will be consistent with the guidelines and principles as described in AS/NZS ISO 31000:2009.

#### 1. Application:

The Risk Management Policy and any associated frameworks, guidelines and protocols will apply across all operations of the City. All employees within the City are encouraged to develop an understanding and awareness of risk and contribute to the risk management process.

#### 2. Definitions:

Risk:

The effect of uncertainty on objectives. (AS/NZS ISO 31000:2009). An effect is a deviation from the expected – positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood.

Risk Management:

Coordinated activities to direct and control an organisation with regard to risk. (AS/NZS ISO 31000:2009)

Risk Management Framework:

Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. (AS/NZS ISO 31000:2009)

### 3. Statement:

The City is committed to ensuring that effective risk management remains central to all its operations while delivering a wide and diverse range of services to its residents and visitors. The management of risk is the responsibility of everyone and should be an integral part of organisational culture and be reflected in the various policies, protocols, systems and processes used to ensure efficient and effective service delivery. The Risk Management Framework will reflect good practice and sound corporate governance and be consistent with the risk management guidelines and principles of AS/NZS ISO 31000:2009.

### 4. Details:

Effective implementation of the Risk Management Framework will ensure that:

- i) Risks that threaten the delivery of services will be identified, recognised and described;
- ii) Risks will be analysed to establish an understanding of their sources and causes and their likelihood and impact should they eventuate;
- iii) Risks will be evaluated to assist in making decisions about risk priorities and treatment plans;
- iv) Risk management processes will be continually reviewed to ensure that controls are effective, new information is gathered, latest changes and trends are identified, successes and failures are recorded, lessons are learned, changes in internal and external context are detected and emerging risks are captured; and
- v) Benefits are realised including;
  - Greater likelihood of achieving objectives;
  - Compliance with legislative and regulatory requirements;
  - Improved stakeholder trust and confidence;
  - Encouragement of decisive leadership rather than crisis management;
  - Better information for improved decision making;
  - Reduced unexpected and costly surprises;
  - Better results from projects and programs; and
  - More effective and efficient allocation of resources.

#### Risk Appetite

Resources available to control risks are limited and the cost of any controls should be considered along with the value of expected benefits. The City's risk appetite will be risk prudent. The City will accept the taking of controlled risks, the use of innovative approaches and the development of new opportunities to improve service delivery provided that the risks are properly identified, analysed and evaluated to ensure that exposures are acceptable and managed accordingly.

#### Availability of the Policy

This Policy will be available on the City's website and Intranet.

DRAFT

---

**Creation Date:** <mmmm yyyy (adopted by Council)>  
**Amendments:** <report ref. (if amendments have been made — not just review)>  
**Related Documentation:** • <*title of document, if applicable*>



# **Draft Risk Management Framework**

**TRIM Ref: 49586**

**May 2013**

# **RISK MANAGEMENT FRAMEWORK**

## **Table of Contents**

	Page
1.0 Introduction	1
2.0 Common Risk Definitions and Explanations	1
3.0 Benefits of Risk Management	2
4.0 Risk Appetite	2
5.0 Principles of Risk Management	2
6.0 Risk Management Process	4
7.0 Risk Categories	6
8.0 Roles and Responsibilities	6
9.0 Key Outcomes	7

### **Appendices**

- A Risk Level Matrix and Assessment Criteria
- B Qualitative Measures of Risk Consequences

## 1.0 Introduction

The City is committed to ensuring that effective risk management remains central to all its operations while delivering a wide and diverse range of services to its residents and visitors. The management of risk is the responsibility of everyone and should be an integral part of organisational culture and be reflected in the various policies, protocols, systems and processes used to ensure efficient and effective service delivery. The Risk Management Framework will reflect good practice and sound corporate governance and be consistent with the risk management guidelines and principles of AS/NZS ISO 31000:2009 (the Standard).

Sound corporate governance requires integrated risk management processes and strategic planning, reporting and performance measurement. The key to successful integration is streamlining the approach to managing risk by ensuring that everyone uses common language and documents their risks using a consistent approach. To effectively embed risk management throughout the City, all employees need to be aware of their responsibilities in relation to managing, communicating and elevating risk.

## 2.0 Common Risk Definitions and Explanations

### Risk:

- The effect of uncertainty on objectives. (AS/NZS ISO 31000:2009)

Note – an effect is a deviation from the expected – positive and/or negative.

- Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood.

### Risk Management:

- Coordinated activities to direct and control an organisation with regard to risk. (AS/NZS ISO 31000:2009)

### Risk Framework:

- Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. (AS NZS ISO 31000:2009)

### Risk Assessment:

This is the part of the risk management process that includes the following three components:

- Risk Identification – process of finding, recognising and describing risks;
- Risk Analysis – Involves developing an understanding of the risk including their causes and sources and the likelihood and consequences should the risk occur; and
- Risk Evaluation – Assists in making decisions about risk priorities and treatments following the risk analysis.

### Risk Monitoring and Review:

- Involves continually reviewing the overall risk management process to ensure that controls are effective, new information is gathered, latest changes and trends are identified, successes and failures are recorded, lessons are learned, changes in internal and external context are detected and emerging risks are captured.

### **3.0 Benefits of Risk Management**

The management of risk is an ongoing process that provides many benefits which include:

- Greater likelihood of achieving objectives;
- Compliance with legislative requirements;
- Improve stakeholder trust and confidence;
- Encourages decisive leadership rather than management of crisis;
- Better information for decision making;
- Reduces unexpected and costly surprises;
- Better results from projects and activities;
- More effective and efficient allocation of resources;
- Balancing opportunity and risk;
- Enhanced accountability and corporate governance; and
- Assists in obtaining insurance cover.

### **4.0 Risk Appetite**

- 4.1 The City seeks to manage risk carefully. Risk appetite is the amount of risk to which an organisation is prepared to be exposed to before it judges action to be necessary. Risk appetite may be described using various terms such as high/medium/low or risk averse, risk prudent or risk tolerant. Resources available to control risks are limited and the amount of risk that the City is prepared to accept at any one time will have a limit.
- 4.2 The City's overall risk appetite is 'risk prudent'. The City should accept the taking of controlled risks, the use of innovative approaches and the development of new opportunities to improve service delivery and achieve its objectives provided that the risks are properly identified, evaluated and managed to ensure that exposures are acceptable.

### **5.0 Principles of Risk Management**

- 5.1 For risk management to be effective, the Standard explains that organisations can achieve effective risk management where their program:

a) creates and protects value

Risk management will contribute to the demonstrable achievement of the City's objectives and improve performance, efficiency in operations and promote good governance and reputation.

b) is an integral part of all organisational processes

Risk management is not a stand-alone activity that is separate from the main activities and processes. Risk Management is part of the responsibilities of management and an integral part of the City's main activities and processes including strategic and corporate planning, project and change management processes and the development of business unit plans.

c) forms part of decision making

Risk management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.

d) explicitly addresses uncertainty

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) is systematic, structured and timely

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) is based on the best available information

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) is tailored to the organisation

Risk management is aligned with the City's internal and external context and its risk profile.

h) takes human and cultural factors into account

Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder the achievement of objectives.

i) is transparent and inclusive

Appropriate and timely involvement of stakeholders, and in particular decision makers at all levels of the organisation ensures that risk management remain relevant and up-to-date. Involvement also allows stakeholders to be properly represented and have their views taken into account in determining risk criteria.

j) is dynamic, iterative and responsive to change

Risk management continually senses and responds to change. As internal and external events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change and others disappear.

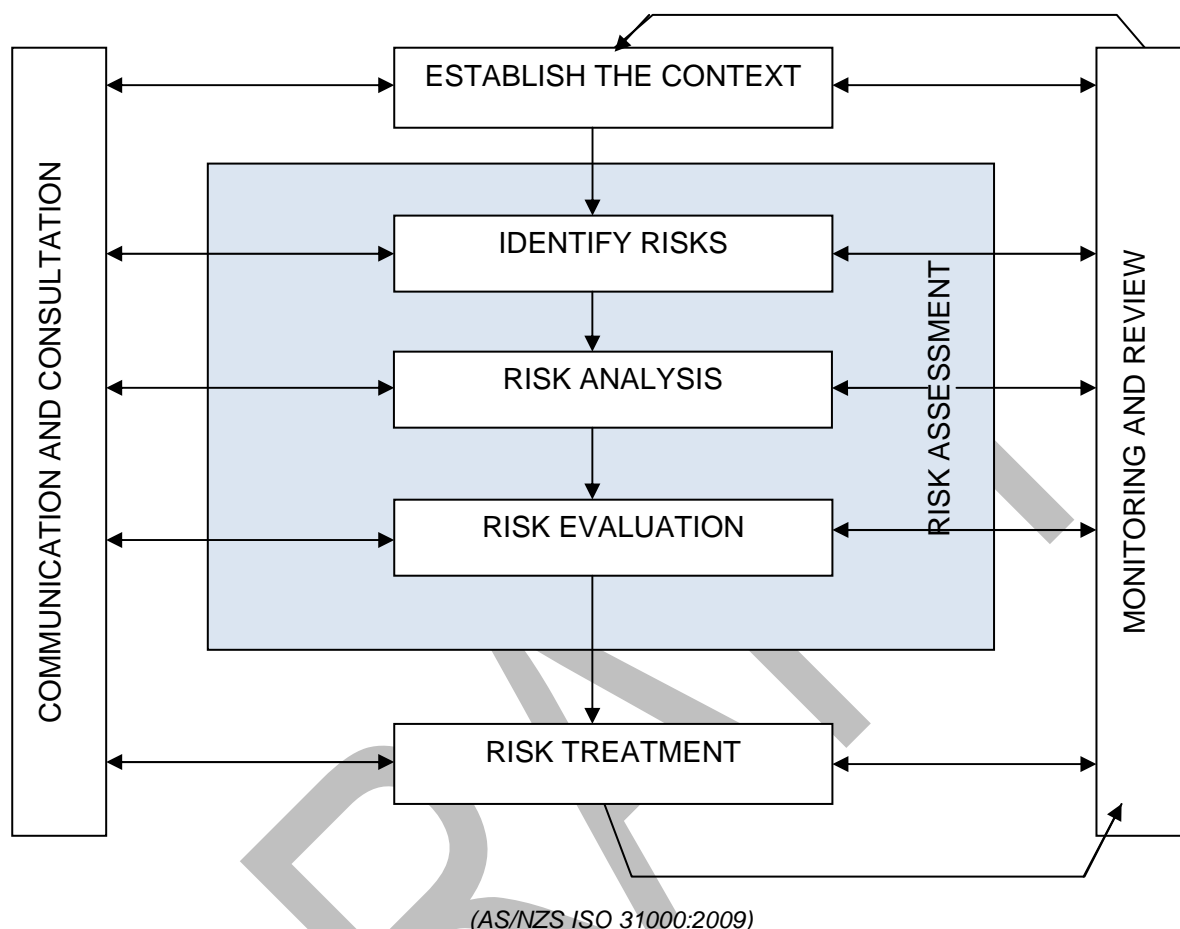
k) facilitates continual improvement of the organisation

Organisations should develop and implement strategies to improve risk management maturity alongside all other aspects of the organisation. A positive risk culture is encouraged where risks are discussed regularly and either accepted as a necessary part of conducting business or actively managed to prevent or reduce the severity of disruptions or impacts to business objectives.



## 6.0 Risk Management Process

Risk Management is about understanding risk tolerance, identifying and assessing what can go wrong in delivering business objectives, what opportunities for improvement or refinements exist and implementing risk treatments when necessary.



### OVERVIEW – RISK MANAGEMENT PROCESS

- 6.1 The risk management process is a series of steps that enable risks to be identified, analysed and treated in the context of the environment in which the City operates. The main elements of the risk management process are as follows:

#### **Communication and Consultation**

Effective internal and external communication and consultation should take place throughout the risk management process to ensure that those accountable for implementing risk management and stakeholders understand the basis on which decisions are made.

#### **Establish the Context**

This identifies the City's objectives and defines the internal and external environment in which it operates. Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered. Understanding the internal context will enable risk management to be aligned with the City's culture, structure, strategies and processes.

<b>Risk Identification</b>	Sources of risk, areas of impact, their causes and potential consequences should be identified. This will generate a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Comprehensive identification is crucial as a risk not identified will not be included in any analysis.
<b>Risk Analysis</b>	This involves the consideration of the causes and sources of risk, their consequences and the likelihood that those consequences can occur. Existing controls and their effectiveness should be taken into account. Risk analysis provides an input to risk evaluation and decisions on the most appropriate risk treatment strategies.
<b>Risk Evaluation</b>	Risk evaluation assists in making decisions, based on the outcomes of the risk analysis, about risk treatment and priorities. Risk evaluation involves comparing the level of risk found during the analysis process with pre-established risk criteria. The risk criteria and the City's risk appetite will help influence the decisions on risk treatment.
<b>Risk Treatment</b>	Selecting the most appropriate risk treatment option involves balancing the cost and efforts of implementation against the benefits derived. A number of treatment options may be considered and can be applied individually or in combination. Risk treatment plans should be prepared which document how the chosen treatment options will be implemented.
<b>Monitor and Review</b>	The Risk Management process should be continually monitored and reviewed to ensure that controls are effective, new information is gathered, latest changes and trends are identified, successes and failures are recorded, lessons are learned, changes in internal and external context are detected and emerging risks are captured.

- 6.2 Risk assessment criteria has been established for analysing and evaluating risks. The criteria is based on the likelihood of the risk occurring and its consequences, a combination of which establishes the overall level of risk. The Risk Level Matrix and Assessment Criteria are included as **Appendix A**.
- 6.3 Qualitative risk criteria for each of the main areas of risk as described at 7.0 are included as **Appendix B**.
- 6.4 The Risk Management Process will be incorporated into the Business Planning Process and risk registers will be included in business plans for each Business Unit.
- 6.5 Following completion of Business Unit Risk Registers the Corporate Risk Register will be updated which will capture any risks assessed as High or Extreme. The Corporate Risk Register will be reported to the Executive Leadership Team annually with designated projects/activities reported quarterly.

## **7.0 Risk Categories**

The areas of risk relevant to the City may be summarised into the following five risk categories.

1. Risk to Human Safety and Wellbeing
2. Legal and Economic Risk
3. Risk to the Environment
4. Risk to the City's Strategic and Governance Position or Reputation
5. Risk to the City's Capacity to Deliver Services

Qualitative Measures of Consequences criteria has been developed in order to assist in the assessment of risk against these categories and is included as Appendix B.

## **8.0 Roles and Responsibilities**

The roles and responsibilities in relation to risk management are:

### **8.1 Audit Committee**

The Audit Committee are responsible for reviewing reports from the Chief Executive Officer on the appropriateness and effectiveness of the City's systems and procedures in relation to risk management, internal control and legislative compliance. The Audit Committee will report to Council the results of that review including a copy of the Chief Executive Officer's report.

### **8.2 Chief Executive Officer**

The Chief Executive Officer is the overall sponsor of the risk management process and will set the tone and promote a positive risk management culture by providing firm and visible support for risk management. The Chief Executive Officer will review the appropriateness and effectiveness of the City's systems and procedures in regard to risk management, internal control and legislative compliance at least once every two calendar years and report the results of that review to the Audit Committee.

### **8.3 Risk Management Taskforce**

The Taskforce provides assurance to the Chief Executive Officer on matters relating to risk management, including the establishment and continuation of steering groups and project teams.

### **8.4 Executive Leadership Team (ELT)**

ELT is responsible for the oversight of the Risk Management Framework, including the review of risk management procedures and policies on an annual basis. It is responsible for setting the tone and promoting a positive risk management culture within the City. ELT maintains oversight of the highest level risks and takes responsibility for ensuring mitigation strategies are being implemented.

## 8.5 Directors

Directors will approve the Business Unit Risk Registers within their Directorate and approve the actions and allocation of resources. Directors will promote a positive risk culture and encourage awareness within their Directorate of responsibilities under the Risk Management Framework. They will ensure the risk register for their Directorate is updated to reflect regular conversations and formal reviews at least quarterly. Directors will ensure timely communication and escalation of emerging or high risks to ELT.

## 8.6 Manager Executive and Risk

Manager Executive and Risk will be responsible for the continual review of the Risk Management Framework and the corporate reporting regime to ensure risk is given adequate consideration.

## 8.7 Managers

Managers will be responsible for ensuring that risk management is integrated into the business and project planning process within their area of responsibility. Managers will maintain a dynamic risk register which will be updated to reflect regular Business Unit discussions. Any high and emerging risks must be escalated to the Director on a timely basis.

## 8.8 Internal Auditor

The internal auditor will develop a risk-based internal audit programme (based on the information gathered in risk registers) and will provide assurance on the efficiency and effectiveness of risk management processes.

## 8.9 Employees

All employees within the City should develop an understanding and awareness of their risks and how they can contribute to the risk management process. It is the responsibility of every employee within the City to manage risks for which they are accountable. All employees are responsible for escalating/communicating risks to their immediate supervisor. Employees are also required to act in a manner that does not place at risk the health and safety of themselves, other employees, residents and visitors to the City.

## 9.0 Key Outcomes

9.1 Risk identification will be integrated into the business and project planning process with the City having an ongoing systematic process for identifying risks.

9.2 Existing systems and procedures to control risks are identified and assessed, critical controls are identified and estimates of likelihood and consequences are based on appropriate information.

9.3 Risks will be evaluated and prioritised using a consistent process with the need for treatment established and prioritised.

9.4 Risk treatment strategies will be developed describing how the treatment options will be implemented.

9.5 There is regular monitoring and review of the risk management process to ensure its relevance.

## APPENDIX A: RISK LEVEL MATRIX AND ASSESSMENT CRITERIA

Risk analysis is an assessment of risks based on a combination of the likelihood of the risk occurring and the severity of the consequences. Risk = Likelihood x Consequence (R = L x C).

### Risk Level Matrix

Likelihood (L)	Almost Certain 5	5	10	15	20	25
	Likely 4	4	8	12	16	20
	Possible 3	3	6	9	12	15
	Unlikely 2	2	4	6	8	10
	Rare 1	1	2	3	4	5
		Insignificant 1	Minor 2	Medium 3	Major 4	Catastrophic 5
		Consequences (C)				

Overall Risk Score = (L x C)	
Score	Description
1 - 5	Low
6 - 12	Moderate
13 - 19	High
20 - 25	Extreme

### Risk Likelihood Matrix

Score	Likelihood	Probability / Frequency
5	Almost Certain	Expected to occur in most circumstances – more than once per year
4	Likely	Will probably occur in most circumstances – will occur once per year
3	Possible	Should occur at some time – at least once every three years
2	Unlikely	Could occur at some time – once every ten years
1	Rare	May occur only in exceptional circumstances – may occur once in a period greater than ten years

### Risk Consequence Matrix

Score	Consequence	Impact
5	Catastrophic	Survival of City threatened, statutory obligations not met, long term damage to reputation, risk to life
4	Major	Long term interruption to major systems, intervention or investigation by other authorities, significant financial impact, serious illness/injury
3	Medium	Major systems inconvenienced, moderate financial impact, external assistance may be required
2	Minor	Non major systems interrupted, low financial impact, some customer inconvenience
1	Insignificant	Negligible impact on systems and service delivery

Qualitative criteria for the main risk areas is also provided as Appendix B to assist in establishing the consequences rating.

## APPENDIX B: QUALITATIVE MEASURES OF RISK CONSEQUENCES

Risk Category	Measures of Consequence				
	Insignificant (1)	Minor (2)	Medium (3)	Major (4)	Catastrophic (5)
<b>Risk to human safety and wellbeing</b>	Injury or illness is minimal with no medical attention required	Injury or illness that may require first aid treatment	Medical attention or ongoing medical treatment  No hospitalisation or long term effects  Potential temporary disability	Multiple serious injuries or illnesses  Permanent disability  Hospitalisation and need for ongoing treatment	One or more deaths
<b>Legal and economic risk</b>	No local law or statutory requirement affected  No impact on City's ability to meet its statutory obligations  No legal implications  Financial impact can be absorbed within existing budget	Minimal legal action with possible minor penalties  Minor impact on City's ability to meet its statutory obligations (can be measured in days)  Low financial impact which may require some budget revision	Moderate legal action  Some delay to City's ability to meet its statutory obligations (can be measured in weeks)  Financial impact requiring budget revision within Business Unit or Directorate	Ongoing legal representation required  Major delay to City's ability to meet its statutory obligations (can be measured in months)  Major financial impact requiring City wide budget review	Intervention by other authorities with legal action initiated  City is unable to meet its statutory obligations in the long term (exceeding one year)  Substantial financial impact requiring major changes in Strategic Community Plan

Risk Category	Insignificant (1)	Minor (2)	Medium (3)	Major (4)	Catastrophic (5)
<b>Risk to the Environment</b>	Incident contained and reversible with no immediate or short term harm to the environment (can be measured in days)	Incident contained with minor short term physical damage or non-toxic nuisance (can be measured in weeks)	Damage to the environment that requires external assistance (can be measured in months)  Some investigation and inspection may be required by external authorities  Some discomfort caused to members of the public	Contamination not contained and extends beyond localised site or point of origin with long term damage (can be measured in years)  Severe discomfort and illness to members of the public  Coordinated response required and investigation instigated by external authorities	Uncontained, irreversible damage with loss of City assets and infrastructure  Resulting in one or more deaths
<b>Risk to the City's strategic and governance position or reputation</b>	Single, unsubstantiated complaint with very low impact  May have a negative impact on an employee or a team	Multiple complaints from a single source  Substantiated low profile single complaint with tentative media interest  May have negative impact on Business Unit	Multiple complaints from multiple sources  Attracting some local media attention with localised damage to reputation  Report or briefing to Council is required  A local law, regulation or policy is required to be developed or amended	Substantiated and significant damage to City's reputation requiring significant efforts to repair  Negative local, regional and state media coverage requiring City's immediate response  Threatens the position of Elected Members  Disciplinary procedures initiated against senior employees	Permanent or long term damage to City's reputation  Negative national media attention  Intervention of other authorities e.g. state government  Commissioners appointed  Enquiry initiated

Risk Category	Insignificant (1)	Minor (2)	Medium (3)	Major (4)	Catastrophic (5)
<b>Risk to the City's capacity to deliver services</b>	<p>Negligible or no impact on critical service delivery</p> <p>Some temporary inconvenience to minor systems and the community</p>	<p>Minor inconvenience to critical systems with short term inconvenience for the community (can be measured in days)</p>	<p>Significant impact on capacity to regularly deliver the service</p> <p>Unable to meet all statutory obligations on time (can be measured in weeks)</p> <p>Review of operational capacity required with possible need for additional staff and resources</p>	<p>Consequences are such that unable to deliver normal services and ongoing inability to meet statutory obligations. (can be measured in months)</p> <p>Ongoing need for additional staff and resources</p> <p>Requires assistance of external agencies</p>	<p>Inability to deliver range of services and failure to meet statutory obligations is ongoing into the foreseeable future (exceeding longer than one year)</p> <p>Ongoing need for additional staff and resources and dependence on external agencies</p> <p>Total loss of capacity due to loss of critical systems and infrastructure</p>