Policy Register

City of Canterbury
City of Cultural Diversity

23-064

Title: Risk Management Policy

Category: Council

Key words: Risk, Risk Analysis, Consequence, Likelihood, Level of Risk, Treatment, Risk Management

File number: R-80-1

Policy owner: Director Corporate Services (Governance)

Authorisation: Council 7 December 1999 (Item 3.1)

Review date: July 2017

Modification history: Risk Management Committee 30 September 2009; Executive Committee May 2014; Minor amendments August 2012; Amended policy approved by Executive 12 June 2014;

Related legislation: Refer to Legislative Compliance Register

Related policies: Fraud and Corruption Control (appendix to Code of Conduct), Work Health and Safety Management System, Privacy Management Plan, Public Interest Disclosure, Information Technology Security, Physical Security

Related procedures: Risk Management Framework

Related forms: Risk Register

Risk Management Plan

Risk Monitoring & Review Schedule

Contents:

1. Purpose

The purpose of this policy is to integrate sound Risk Management practices and procedures into the culture, business practices and processes of Council. Our policy adopts the risk management approach and general methodology established in the Australia/New Zealand International Standards Organisation Risk Management Standard (AS/NZS ISO 31000:2009)

2. Objectives

Our objectives are to:

- create an environment where employees have a key role in managing risk;
- promote a program which contributes to improved organisational performance by managing risk proactively;
- be prudent in safeguarding Council assets – people, finances, information and property;
- contribute to the cost effective and timely achievement of organisational goals; and
- achieve a common risk management process which is applied consistently across the Council.

3. Scope

Risk Management is built into existing decision making structures and processes such as strategic management, operational and project planning, and program review to ensure it is part of day-to-day activities.

4. Definitions

Risk – is the chance of something happening that will have an impact on objectives.

Risk Analysis - is the identification of the consequences (impact) should an event occur and the likelihood (possibility) of the event occurring.

Consequence - is the direct effect of an event, incident or accident. It can be expressed as a health effect (e.g., death, injury, and exposure), property loss, environmental impact or other impact.

Likelihood - is expressed as either the frequency or probability of an event occuring. Frequency is the rate at which events occur over time (e.g., events/year, incidents/year, deaths/year, etc.). Probability is the rate of a possible event expressed as a fraction of the total number of events (e.g., one-in-a-million, 1/1,000,000, or $1X10^{-3}$).

Level of Risk - is a grading, establish by combining the results of the Risk Analysis, against a predetermined matrix.

Treatment – is the process of selecting and implementing measures to reduce the likelihood or consequences (or both) of a particular event or risk occurring.

Risk Management - in its simplest form is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

5. Principles

The principles of the Policy come directly from the standard and will be achieved by:

- Establishing organizational principles that ensure the success of the Risk Management Program.
- Establish a Management Framework in which the Risk Management Process function, including:
  - Mandate and Commitment,
  - Design a Framework for Managing Risks,
  - Implementation Risk Management,
  - Monitoring and Review of the Framework, and
  - Continual Improvement of the Framework.
- Ongoing implementation of the Risk Management Process, including:
  - Communication and consultation with all major stakeholders with regard to the management of risk in Council.
  - Establishing the Context to better understand the environment in which the risk assessment is being prepared.
  - Identifying Risks which do or may have an impact of our capacity to deliver services.
  - Analysing Risks to assess the level of impact the eventuality of an event occurring will have on our services.
  - Evaluating Risks to decide if they are acceptable or unacceptable and to establish a priority for treating them.
  - Treating Risks by, avoiding, reducing, transferring or accepting them.
  - Monitoring and Reviewing all risk by developing a review program.
  - Recording the Risk Management Process and all documents associated with it to ensure transparency and audit ability.

6. Responsibilities

The **General Manager** has ultimate responsibility for good corporate governance, including ensuring risk management operates effectively across the organisation.

Directors and Managers are responsible for the maintenance of sound risk management practices within their area of responsibility to ensure the delivery of effective, efficient and economically sound business outcomes.

The **Internal Audit Committee** has responsibility to:

- set and review 3 year internal audit program and priorities taking account of risks identified by the organisation;
- consider internal audit reports;
- consider risk management reports; and
- monitor implementation of recommendations.

The **Risk Management Committee** has responsibility to:

- oversee the alignment of risk management strategies with our corporate objectives;
- promote best practice in risk management and internal controls;
- consider risk reports and endorse appropriate risk treatment recommendations;
- monitor progress of risk treatment strategies;
- establish and review Council's risk appetite; and
- monitor business unit implementation of risk management strategies.

The **Group Manager Governance** monitors the efficiency, effectiveness and economy of Risk Management practices and risk mitigation strategies and to report deficiencies to the General Manager through the Director Corporate Service via the Risk Management Committee.

The **Risk Management Coordinator's** role is to:

- develop and continually improve the Risk Management Policy, Framework and Process to ensure it meets Australian Standards and our requirements;
- facilitate the planning, direction and management of the risk management function across Council;
- facilitate risk assessments and risk profiling from a holistic approach;
- record, maintain and monitor results of risk assessments; and
- provide input to the Council's learning programs which will give management and staff training to improve risk management skills.

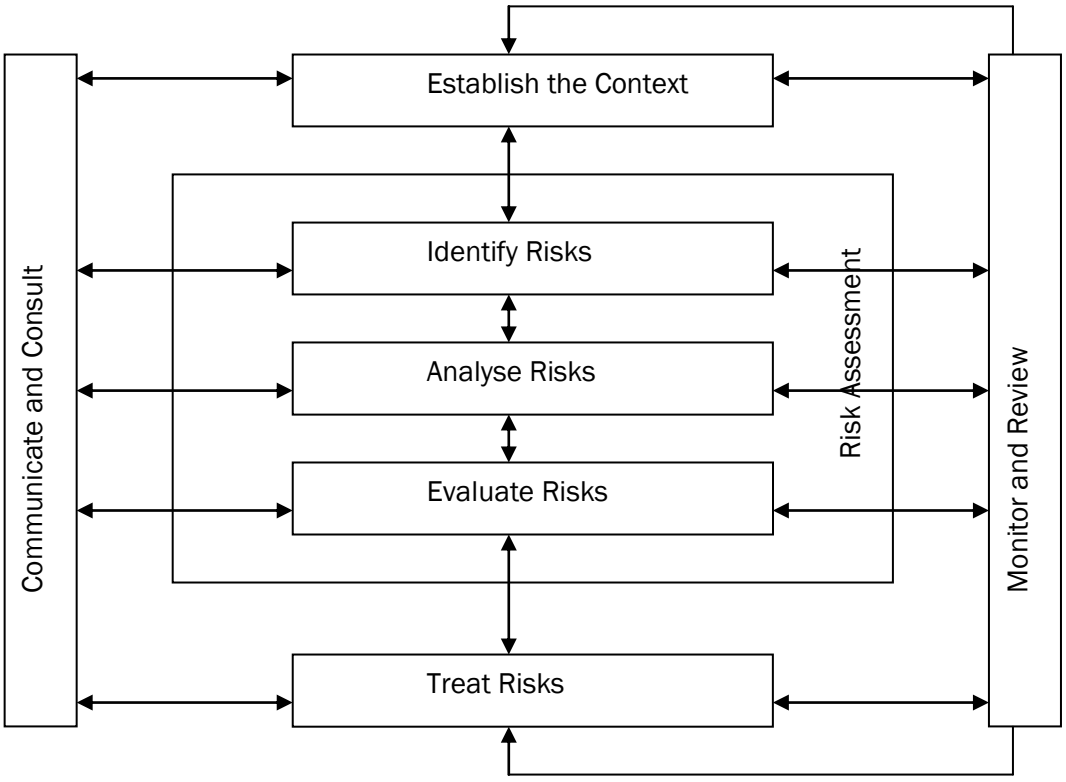
Responsibility is assigned to operational managers and employees to ensure information affecting risk is collected as part of local planning and reported to the Risk Management Committee via the Risk Management Coordinator.

7. Procedures

The procedures in this document are a summary of those in the Risk Management Framework.

The Risk Management Process

(The Council Risk Management model is adopted directly from the AS/NZS ISO 31000:2009)



The Risk Management Process

Summary

The process for managing risk has eight components which are drawn directly from AS/NZS ISO 31000:2009.

Step 1 – Communicate & Consult

This is an important component at each step of the Risk Management Process. It is used to ensure all stakeholders have appropriate and adequate information about the program and allows for an exchange of information and opinions. It seeks to:

- develop trust;
- engage stakeholders;
- set clear expectations;
- improve people's understanding of risks and the risk management process;
- ensure that the varied views of stakeholder are considered; and
- ensure that all participants are aware of their roles and responsibilities.

Step 2 – Establish the Context

The initial process is defining the basic parameters within which risks must be managed. This sets the scope for the rest of the Risk Management Process.

Step 3 – Identify Risks

Effective risk identification involves examining all sources of risks and the perspective of all stakeholders, both internal and external.

It is important to identify each risk and its source so that the analysis can consider the likelihood of it occurring and its possible consequences. This can be achieved by:

- document review such as policies, procedures, legislation, process design maps, audit reports, annual reports etc;
- flowcharts and dependency analysis;
- surveys, questionnaires;
- Strengths, Weaknesses, Opportunities, Threats (SWOT) and Political, Economic, Social, Technical, Legal Environmental (PESTLE) analysis;
- field inspections;
- audits (external and internal);
- Hazard and Operability HAZOP studies and Failure Modes Effects Analysis (FMEA);
- interviews and group discussions with stakeholders; and
- reviewing similar operations in like organisations.

Step 4 – Analyse Risk

This step involves the analysis and rating of each risk. The level of risk is the product of the relationship between the likelihood of the event occurring (frequency and probability) and the consequence (impact or magnitude) of the risk if it occurs.

There are three methods used to assess the level of risk:

1) **Quantitative Risk Analysis** are based on actual data or determined by analytical techniques.

2) **Qualitative Risk Analysis** uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. The assessment is based on personal judgments made by an individual but preferably by group consensus on the likelihood and consequence of an event occurring.

3) **In Semi-Quantitative Analysis**, qualitative scales are given values. The objective is to provide a more expanded ranking scale then is usually achieved in qualitative analysis.

Step 5 – Evaluate Risks

Risk evaluation is the process of deciding whether risks are acceptable of unacceptable. A risk is acceptable if is has adequate and effective risk mitigation controls in relation to the benefits and opportunity presented by taking the risk.

Step 6 – Treat Risks

This step is about reviewing the options for treating unacceptable risks and deciding on an appropriate course of action. This may include:.

- Terminate the risk by deciding not to proceed with the policy/program/project or activity.
- Treat the level of risk by reducing either the likelihood, consequence or both through the introduction of management or internal controls.
- Transfer the risk by shifting responsibility to another party. Risk can be transferred by contract, insurance, legislation or administrative process.
- Tolerate and retain the risk after careful analysis of the cost of treatment. The decision not to reduce the level of risk should be carefully documented. Ongoing monitoring of accepted risks should be undertaken in case circumstances change.

Step 7 - Monitor and Review

When risks have been identified and controls put in place it is important to monitor and review the ongoing effectiveness of the mitigation strategies. Factors which may affect the likelihood and consequences may change, as may factors that affect the suitability or cost of treatment options.

Step 8 – Record of Risk Management Process

To ensure transparency in decision making and to enable effective reviews to be undertaken all assumptions, methods, data sources, analyses, results and reasons for decisions must be recorded and maintained.

8. Documents

The following documents are to be maintained as part of the Risk Management process:

Risk Matrix: is used during risk assessment to define the various levels of risk as a produce of the harm probability categories and harm severity categorise. This is a simple mechanism to increase visibility of risk, allow them to be evaluated with all other risks and assist in management decision making.

Risk Register: is a record of risks for a particular program, process or function. The register includes the consequences and likelihood of an event occurring, the adequacy of existing controls and the level of risk.

The Risk Management Coordinator will be responsible for maintaining the Enterprise Risk Register and ensuring that a copy is provided to and reviewed by the Risk Management Committee at each meeting.

All managers will receive a Team Risk Register relevant to their area of responsibility. The managers will be responsible for ensuring it continues to be accurate and relevant. Any changes to the register must be discussed with the Risk Management Coordinator.

Risk Management Plan: is a record of all approved Risk Treatment activities with details of priority, team or individual responsible and delivery dates.

The Risk Management Plan will be created by the Risk Management Coordinator with details obtained from the Risk Register. The completed plans will be provided to the Executive and Risk Management Committee for review.

To effectively align risk management with Corporate Strategic Planning, a copy of the Enterprise Risk Management Plan will be provided to the Manager Corporate Strategy for inclusion in Operating Plans.

Monitoring & Review Schedule: is a plan for the program of monitoring and review activities that will be undertaken to ensure the continued relevance and accuracy of Risk Management within the Council.

The schedule will be developed by the Risk Management Coordinator in consultation with the Executive, Risk Management Committee and Group Manager Governance. Completed schedules will be retained for audit purposes.