



## COUNCIL LEAD POLICY

**POLICY TITLE: RISK MANAGEMENT**

**Minute Ref:**

**Date of Adoption: 28<sup>th</sup> October 2014 (Finance & Risk Committee)**

### 1. POLICY OBJECTIVES

To provide a consistent process to enhance efficient operations, effective processes and successful strategies that increase the likelihood of achieving the best outcomes for the city and the Council by:

- ensuring risk-based information is available to support good decision-making
- providing assurance that risks are being appropriately addressed and managed, and
- ensuring compliance with applicable legislation and regulation.

### 2. PRINCIPLES

Council's approach to risk management is consistent with the Joint Australian New Zealand International Standard *Risk management – Principles and guidelines* (AS/NZS ISO 31000:2009). That Standard provides the following principles of risk management:

- Risk management creates and protects value
- Risk management is an integral part of all organisational process
- Risk management is a part of decision making
- Risk management explicitly addresses uncertainty
- Risk management is systematic, structured and timely
- Risk management is based on the best available information
- Risk management is tailored
- Risk management takes human and cultural factors into account
- Risk management is transparent and inclusive
- Risk management is dynamic, iterative and responsive to change
- Risk management facilitates continual improvement of the organisation

### 3. DEFINITIONS

**Control** is a process, policy, device, practice or other action that reduces the likelihood of a risk event occurring or reduces the potential consequence of that risk event before the risk event occurs.

**Council** means the entity known as the Tauranga City Council and includes the governing body and the organisation

**Governing body** means the mayor and councillors

**Mitigation** is a process, policy, device, practice or other action that is intended to reduce the consequence of a risk event after the risk event has occurred.

**Organisation** means the operations, processes and staff of Tauranga City Council led by the Chief Executive

**Residual risk** is the risk remaining after risk treatment. (AS/NZS ISO 31000/2009)

**Risk** is the effect of uncertainty on objectives. (AS/NZS ISO 31000/2009)

**Committee responsible for risk** means the Finance and Risk Committee established by the Mayor on or before 19 November 2013 in accordance with section 41A(3)(b) of the Local Government Act 2002, or a subsequent Committee of Council established with similar roles, responsibilities and powers.

**Risk event** is an occurrence or a change in a particular set of circumstances that gives rise to, or modifies, a risk.

**Risk management** is the coordinated activities to direct and control an organisation with regard to risk. (AS/NZS ISO 31000/2009)

**Risk management framework** is the combined suite of tools and processes, including this policy and supporting procedures, by which Council manages risk.

**Risk management plan** is a schedule that records risks and the controls, mitigations, risk treatments, and accountabilities associated with those risks.

**Risk register** is the same as a 'risk management plan'.

**Risk treatment** is the process to modify risk. (AS/NZS ISO 31000/2009)

### 4. BACKGROUND

#### 4.1 Objectives

Risks are defined in relation to relevant objectives.

At the highest level, Council's objectives are expressed through its desired community outcomes of:

- a talented and innovative city full of opportunity
- a city with heart and soul
- a city of great spaces, places and environments

... and through the organisational vision of becoming:

- the best local authority in Australasia.

At subsidiary levels, risks will be defined in relation to relevant objectives at that level.

## 4.2 Risks

Risks can be positive or negative.

Risks can also be 'risks to Council' or 'risks to the city'.

Positive risks, or opportunity risks, should be embraced, in a cost-effective manner, to the extent that they help Council or the city to meet its objectives.

Negative risks should be managed in a cost-effective manner so that they do not detract from Council or the city meeting its objectives.

In tabular form these concepts can be shown as follows:

City risks	3 Understanding risks for the city and assessing Council's role in managing those risks	4 Understanding opportunities for the city and assessing Council's role in developing those opportunities
Council risks	1 Understanding and managing risks for Council and its immediate stakeholders	2 Understanding and exploiting opportunities for Council
	Negative risk	Positive risk

Council's initial approach will be to focus on quadrant 1 while remaining aware of the responsibilities and possibilities under quadrants 2, 3 and 4.

Council has established a comprehensive risk management framework that principally focuses on quadrant 1 risks. This approach will be reviewed in time.

## 5. POLICY STATEMENT

### 5.1 Commitment to risk management

Council recognises that early and systematic identification, analysis and assessment of risks and the development of plans for controlling and mitigating risk are necessary to achieve its desired objectives.

As such, Council is committed to identifying, analysing, assessing and appropriately managing the risks to its objectives.

Risk management is the responsibility of everyone.

Council encourages intelligent and informed risk-taking and risk-acceptance in pursuit of its objectives.

### 5.2 Identification of risks

All staff members are empowered, and expected, to identify and communicate risks. Identified risks will be recorded in a risk management plan.

Where, for whatever reason, direct reporting lines are not able to be used to communicate identified risks, alternative methods will be made available.

These will include, but not be restricted to, direct notification to the Risk Specialist, General Managers or the Chief Executive.

### **5.3 Analysis of risks**

Risks will be analysed to determine potential causes, the likelihood of occurrence, and the potential consequences if they do occur.

The causes, likelihood and consequence will be recorded in a risk management plan.

In accordance with the principle that risk management is tailored, the analysis of risks will reflect the relevant objectives of the Council, organisation, group, division, team or project.

For the high-level 'corporate risk management plan':

- The likelihood of a risk event occurring will be assessed in accordance with the Likelihood Table included as [Attachment 1](#).
- The potential consequences if a risk event occurs will be assessed in accordance with the Consequence Table included as [Attachment 2](#).
- The assessments of the likelihood of a risk event occurring and the potential subsequent consequences will be considered together in accordance with the Risk Matrix included as [Attachment 3](#).

The analysis of risks at subsidiary levels will be undertaken in a manner consistent with the above but may be tailored to suit the relevant circumstances.

### **5.4 Evaluation of risks**

Analysed risks will be evaluated against criteria to determine whether a risk is tolerable in its current state or whether further action is required.

The evaluation of risks will consider established risk tolerances for such risks, as well as any risk-specific factors.

In the first instance the evaluation of risks will include reference to the Risk Response table included as [Attachment 4](#).

### **5.5 Treatment of risks**

Where residual risk is considered to be too high, risk treatments will be applied to reduce the residual risk to an acceptable level.

In considering risk treatments consideration will be given to both the costs and effort involved in the treatment and the potential benefit from the risk reduction.

Risk treatment can involve:

- avoiding a risk by deciding not to start or continue with the activity that gives rise to the risk
- taking or increasing risk in order to pursue an opportunity
- removing the risk source
- changing the likelihood of the risk occurring
- changing the consequence if the risk occurs

- sharing the risk with another party or parties, or
- retaining the risk by informed decision.

## 5.6 Recording of risks

Risks, controls and mitigations will be recorded in a risk management plan.

A high level organisation-wide 'corporate risk management plan' will be maintained to record and report on risks of Council-wide significance.

Subsidiary risk management plans will be prepared as appropriate throughout the organisation. These may include, but will not be limited to:

- group risk management plans
- activity risk management plans
- division or team risk management plans
- asset risk management plans
- specialist risk management plans (for example, health and safety)
- project risk management plans, and
- any other risk management plan relevant to helping Council achieve its objectives.

## 5.7 Reporting of risks

Identified risks, and the associated controls, mitigations and accountabilities, will be reported in accordance with the Risk Response table included as Attachment 4.

Risk management plans will be reported regularly to both the Executive Leadership Team and the Committee responsible for risk.

## 5.8 Accountability for risks

Specific accountability for each risk, control and mitigation will be identified and recorded in a risk management plan.

## 5.9 Roles and responsibilities

Assigning specific responsibilities to specific roles provides clarity and strengthens the overall risk management framework.

Governance	Responsibility
Council	To be assured that a risk management framework is in place and that risks are being appropriately managed.
Committee responsible for risk	Subject to the governing body's delegated authority, the Committee responsible for risk has responsibility to: <ul style="list-style-type: none"> <li>• approve the risk management framework</li> <li>• consider matters related to the quality assurance and internal controls in the organisation including by enquiry and monitoring of risk matters</li> </ul>

	<ul style="list-style-type: none"> <li>advise the governing body on matters of risk and provide objective advice and recommendations for the governing body's consideration</li> </ul>
<b>Management</b>	<b>Responsibility</b>
Chief Executive	<p>Approve the risk management framework and recommend it to the Committee responsible for risk</p> <p>Lead and promote a risk aware culture across the organisation</p> <p>Implement the risk management framework across the organisation</p>
Executive Leadership Team	<p>Endorse the risk management framework and champion it to the organisation</p> <p>Monitor effective implementation of the risk management framework across the organisation</p> <p>Receive and consider risk management plans on a monthly and quarterly basis</p> <p>Receive and consider other risk-related reports on an as-required basis</p> <p>Provide direction on risk tolerance at a general and risk-specific level</p> <p>Periodically review the risk management framework to ensure it remains appropriate</p>
General Managers	<p>'Own' risks relevant to, or arising from, their groups</p> <p>Lead and promote a risk culture within their groups</p>
Risk Forum	Assist the Risk Specialist to manage the interface between subsidiary risk management plans and the high level 'corporate risk management plan'
Risk Specialist	<p>Develop and maintain the risk management framework</p> <p>Facilitate the population and ongoing review of the high level 'corporate risk management plan'</p> <p>Manage the interface between subsidiary risk management plans and the high level 'corporate risk management plan'</p> <p>Advise on potential risk treatments for identified risk</p> <p>Consider and, where necessary, challenge the risks, controls, mitigations and accountabilities included (or not included) in risk management plans across the organisation</p> <p>Lead the roll-out of the risk management framework across the organisation</p> <p>Train and assist operational managers and leaders to implement the risk management framework in their divisions and teams</p> <p>Lead the integration of risk management principles into other Council decision-making processes</p>

Operational managers and leaders	Develop, populate and manage the risk management plan for their division or team in accordance with the risk management framework  'Own' risks relevant to, or arising from, their divisions or teams  Lead and promote a risk aware culture within their groups
Staff & contractors	Provide support in identifying risks  As appropriate, 'own' risks, controls or mitigations

## 6. RELEVANT DELEGATIONS

The Chief Executive or his/her nominee has delegated authority for the implementation of this policy.

## 7. REFERENCES AND RELEVANT LEGISLATION

Joint Australian New Zealand International Standard *Risk management – Principles and guidelines* (AS/NZS ISO 31000:2009).

- Attachments:
- 1 Likelihood Table
  - 2 Consequence Table
  - 3 Risk Matrix
  - 4 Risk Response Table

# Attachment 1

## Categories of likelihood

Almost certain	5	90% or greater chance of occurring in next 12 months Expected to occur in 9 of next 10 years Certain to occur at least once in next 5 years It would be unusual if this didn't happen
Likely	4	60% to 90% chance of occurring in next 12 months Expected to occur in 7 of next 10 years Certain to occur at least once in next 5 years Will occur more often than not
Possible	3	25% to 60% chance of occurring in next 12 months Expected to occur in 4 of next 10 years Likely will occur at least one in next five years (>80% chance) Not likely, but don't be surprised
Unlikely	2	2% to 25% chance of occurring in next 12 months Expected to occur a maximum of once every 5 to 20 years 50% chance of occurring in next 5 years A surprise, but not beyond the bounds of imagination
Rare	1	Up to 2% chance of occurring in next 12 months Could occur once every 50 or more years Less than 10% chance of occurring in next 5 years Will only occur in exceptional circumstances

## Categories and descriptors of consequence

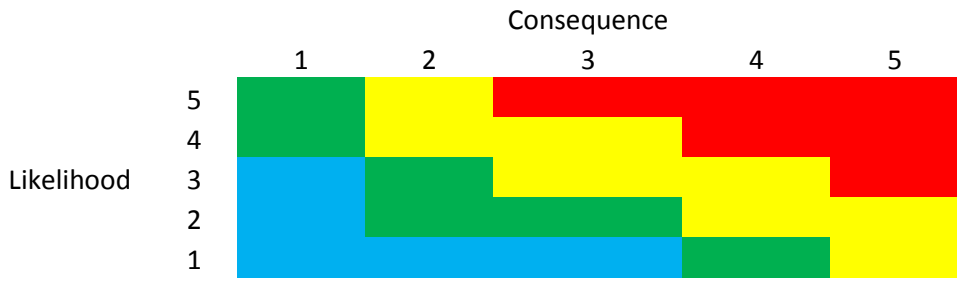
## Attachment 2

	1	2	3	4	5
	Less than minor	Minor	Moderate	Major	Extreme
Achievement of strategic outcomes <sup>1</sup>	No impact on strategic impacts	Inconvenience or delay in achieving strategic outcomes	Significant difficulty introduced to achievement of strategic outcomes Lost opportunity to contribute positively to one or more strategic outcomes	Failure to achieve a specific strategic outcome Lost opportunity to significantly advance a specific strategic outcome	Failure to achieve multiple strategic outcomes Lost opportunity to significantly advance multiple strategic outcomes
Financial	Financial impact of less than \$50,000  Financial impact of less than 1% of the group's total opex <sup>2</sup>	Financial impact of between \$50,000 and \$250,000  Financial impact of between 1% and 2% of the group's total opex <sup>2</sup>	Financial impact of between \$250,000 and \$1 million  Financial impact of between 2% and 5% of the group's total opex <sup>2</sup>	Financial impact of between \$1 million and \$10 million  Financial impact of between 5% and 10% of the group's total opex <sup>2</sup>	Financial impact of more than \$10 million  Financial impact of more than 10% of the group's total opex <sup>2</sup>
Health and Safety (customers, staff, contractors)	Minor injury, first aid not required	First aid or minor treatment	Medical treatment required	Serious harm, for example broken bones, hospitalisation	Loss of life; multiple serious harms; permanent severe disability
Service delivery to community	Short-term reduction in service delivery which is easily restored and does not compromise the community's health and wellbeing	Reduced service delivery that does not compromise the community's health and wellbeing	Key service not available to some of the community for ten hours or more  Continued service degradation for two days or more	Key service not available to a significant portion of the community for two days or more  Continued severe service degradation for one week or more	Key service not available to a large proportion of the community for one week or more  Continued severe service degradation for one month or more
Organisational capability and capacity	Temporary problem with organisational capability resulting in no impact on external service delivery	Loss of organisational capability in some areas resulting in sub-optimal support to external delivery activities	Organisation unable to function for less than 10 hours  Serious reduction in organisational capability for one week or more	Organisation unable to function for more than 10 hours  Serious reduction in organisational capability for two weeks or more	Organisation unable to function for more than two days  Serious reduction in organisational capability for one month or more
Reputational	Negative feedback from individuals  Short-term 'letters to the editor' (or online equivalent) commentary	Short-term loss of confidence among small sections of the community Regional adverse political or media comment for one or two days Sustained 'letters to the editor' (or online equivalent) commentary in usual sources	Short-term and manageable loss of community confidence Regional adverse political or media comment for more than two days Significant social media commentary or campaign from new sources	Loss of community confidence requiring significant time to remedy National adverse political or media comment for more than two days Regional adverse political or media comment for more than one week Requirement for (televised) public explanation	Insurmountable loss of community confidence National adverse political or media comment for more than one week Requirement for (televised) public apology or defence Adverse comments or questions in Parliament
Legislative / regulatory compliance	One-off minor regulatory or legislative non-compliance with no direct impact on the community's health or wellbeing	One-off minor regulatory or legislative non-compliance with potential impact on the community's health or wellbeing	Complaint to the Ombudsman, Auditor-General or other statutory office Multiple related minor non-compliances due to an underlying systemic issue Significant breach or non-compliance resulting in regulatory scrutiny	Significant breach or non-compliance, or multiple breaches or non-compliances, resulting in regulatory action and/or restrictions on Council activities	Court proceedings or criminal action for breach or non-compliance; potential for imprisonment of elected member or staff Judicial review on a matter of rates or other funding, or on a matter with significant financial impact.

<sup>1</sup> Strategic outcomes comprise the externally-focused community outcomes (a talented and innovative city full of opportunity; a city with heart and soul; a city of great spaces, places and environments), the internally-focused organisational vision (the best local authority in Australasia), and specific cornerstone projects supporting the community outcomes or organisational vision.

<sup>2</sup> 'Group' in this context means the organisational groups, each reporting through a General Manager (or equivalent) to the Chief Executive.

### Risk Matrix



## Attachment 4

Overall risk rating	Action	Reporting
<p style="text-align: center;"><b>Extreme</b></p>	<p>Urgent and active management required.</p> <p>Risk treatment plan must be implemented immediately to reduce the risk exposure to an acceptable level.</p> <p>Regular reporting required.</p>	<p>Immediate notification to relevant General Manager.</p> <p>Advise Risk Specialist to allow tracking of risk.</p>
<p style="text-align: center;"><b>High</b></p>	<p>Management attention is required.</p> <p>Risk treatment plan required.</p> <p>Regular reporting required.</p>	<p>Notification to relevant General Manager.</p> <p>Advise Risk Specialist to allow tracking of risk.</p>
<p style="text-align: center;"><b>Moderate</b></p>	<p>Management responsibility to monitor.</p> <p>Focus on ensuring internal controls are effective and monitoring the ongoing risk.</p>	<p>Included on management-level risk register.</p> <p>Risk Specialist to review risk registers periodically.</p>
<p style="text-align: center;"><b>Low</b></p>	<p>Can be monitored using routine practices.</p> <p>Focus on ensuring internal controls are effective</p>	<p>Included on management-level risk register.</p> <p>Risk Specialist to review risk registers periodically.</p>