RISK MANAGEMENT POLICY

DATE ADOPTED: 5 DECEMBER 2017

TE WAIROA
WAIROA DISTRICT

PERSON RESPONSIBLE:	Chief Executive Officer	**COMMITTEE RESPONSIBLE:**	Finance, Audit & Risk Committee
CATEGORY:	Office of the Chief Executive	**STATUS:**	FINAL
DATE POLICY ADOPTED:	5 December 2017	**APPROVAL BY:**	Council
REVIEW PERIOD:	Annual review by FAR Committee	**NEXT REVIEW DUE BY:**	December 2018
DATE PREVIOUSLY ADOPTED:	N/A	**REVISION NUMBER:**	0

1. Purpose

Risk management is recognised as an integral part of good management practice and is an important aspect of corporate governance. The purpose of this policy is to explain the Council's underlying approach to strategic risk and risk management, both financial and non-financial.

This document outlines the policy, strategy, guidelines, process and approach to risk management to ensure that sound risk management practices are incorporated into the Council's planning and decision-making processes are aligned with the *ISO31000: 2009 Risk Management Standard*. The Risk Management Policy is the governing framework with respect to the Council's risk management profile and where other frameworks exist to manage categories of risk, these principles, expectations, processes and approach must be adopted.

2. Organisational scope

This is a Council-wide policy overseen by the Chief Executive Officer. Staff, contractors, and elected members have a shared role to play in the identification, reporting and management of risk through risk management processes being integrated with planning processes and embedded in management activities.

3. Definitions

The following definitions are sourced from AS/NZS ISO31000.2009.

Risk	Effect of uncertainty on objectives
Risk assessment	The overall process of risk identification and evaluation.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk management process	Systematic application of management policies, procedures and practices to activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risks: • communicate and consult – with internal and external stakeholders at all stages of the risk

	consideration and decision-making processes; • establish the context – determine the criteria against which the risk is to be evaluated and managed, considering both internal and external stakeholders; • identify the risk – consider the range of potential likelihood and consequence of the occurrence of risk events; • analyse the risk – consider the range of potential likelihood and consequence of the occurrence of risk events; • evaluate the risk – by comparison with pre-established criteria, and consideration of the balance between benefits and adverse outcomes; • treat the risk – develop cost-effective strategies, options, and action plans for the treatment of risks that show both positive and negative outcomes; • monitor and review the risk – monitor the effectiveness of all steps, and measures taken in order to achieve improvements, to react to changes in circumstances, and to ensure priorities are still relevant; • record the process – all relevant data pertaining to decision-making should be recorded, to satisfy legal and business needs, and to serve as a database for reuse. The scale and maintenance of such records should be cost-effective.

Other definitions:

Consequence	The impact on an organisation should an event occur.
Likelihood	The potential of an event occurring.
Risk rating	The level of severity applied to a risk based on its impact to Council, the community and other stakeholders.
Risk analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or criteria.
Risk assessment	The overall process of risk analysis and risk evaluation.
Risk mitigation	A selective application of appropriate control measures, techniques and management principles to reduce either the likelihood of an occurrence or its consequences or both. Risk can never be totally eliminated.
Risk owner	Person or entity with the accountability and authority to manage a risk.
Risk register	Record of information about identified risks.
Risk control	That part of risk management which involves the implementation of policies, standards, procedures and physical changes to a thing, work process or system of work to eliminate or minimise both adverse and moderate

	risks.
Risk appetite	The level of risk that Council is prepared to accept, before action is deemed necessary to reduce it. Acceptable risk levels represent a balance between the potential benefits of calculated risk and the threats that it inevitably brings.

4. Policy content and guidelines

Wairoa District Council (WDC) is actively committed to the effective and efficient management of risk that realises opportunities for gains, whilst minimising losses. Council seeks to identify all key risks that could impact on the viability of its responsibilities and operations and has contingencies in place to avoid, minimise, mitigate and/or accept risks within its sphere of control or influence.

By this commitment to risk management, WDC aims to achieve the following objectives:

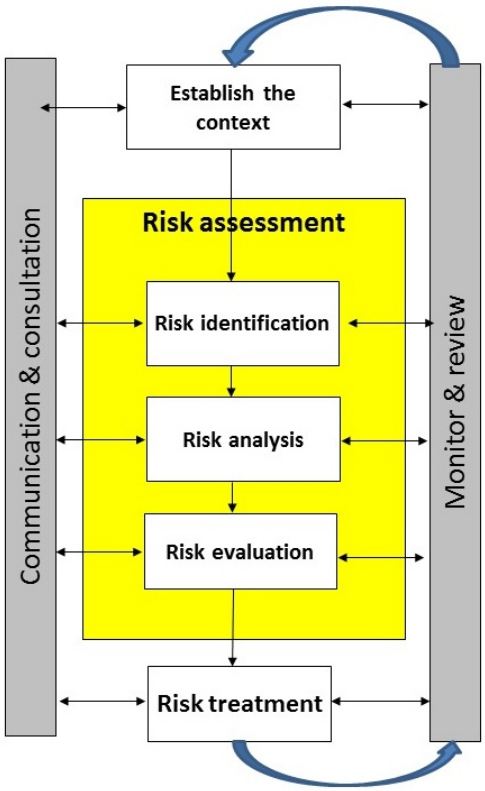
a) Define risk in the context of Council;
b) Articulate Council's commitment to risk management;
c) Introduce the fundamental principles and measures of risk;
d) Promote and support risk identification management and hazard identification practices and priorities throughout the organisation;
e) Provide broad guidance to elected members, Council's managers, employees, contractors and other stake-holders which will be relevant to their risk management responsibilities with the following sub-outcomes:
    - A more confident and rigorous basis for decision-making and planning
    - Stronger identification of opportunities and negative consequences
    - Obtaining value from uncertainty and variability
    - Environmental protection
    - Effective allocation and use of resources
    - Improved incident management, reducing loss and risk costs
    - Improved stakeholder confidence and trust
    - Improved compliance with legislative requirements
    - Better corporate governance
    - Contingency planning for foreseeable emergency situations;
f) Recognise that successful risk management relies on input from all employees;
g) Recognise that successful risk management involves the community, ratepayers, and other external stakeholders of Wairoa;
h) Protect Council's image.

4.1 Approach to risk management

For the Risk Management process to be efficient and effective within Council, it must be:

- an integral part of management;
- embedded in the culture and practices; and
- tailored to the business planning and processes of the organisation

The process comprises a number of steps as recommended by ISO AS/NZS 3100.2009. The steps are detailed in the flowchart below:



Communication and Consultation

Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process.

External stakeholder communication informing and consulting on:

- the Councils approach to risk management;
- effectiveness of the council's risk management approach;
- and gathering feedback as appropriate on risk management including risk appetites and fiscal choice.

Internal stakeholder communication including:

- communicating the risk management processes;
- gathering feed-back in relation to risk management and processes;
- ensuring accountability of roles and responsibilities are clearly understood in relation to the risk management process.

Step 1: Establishing the Context

The establishment of the context is an integral element within the process of risk management as it establishes and defines the various environments in which risk is to be considered, assessed and managed.

The level of contextual relevance should be considered on;

- an external context - which is the extent to which the Council's external environment will impact on its ability to achieve its corporate objectives;
- an internal context – which is about understanding the internal operating environment;
- the context of the risk management process – establishment of the objectives, strategies, scope;
- defining the risk criteria – the organisation should define criteria to be used to evaluate the significance of risk.

Step 2: Identify Risks

Risk identification is a key step to ensure the risk exposures which Council may be subject to are recorded. This sets the foundation for the establishment of effective and efficient risk mitigation, control and review.

All risks must be linked to Council outcomes, strategies and plans and form part of Councils overall vision for the city, sphere of responsibility and/ or influence.

The key elements of Councils risk identification processes are:

- the cyclical risk assessments undertaken by Council's internal and external auditors;
- risk assessments undertaken within individual divisions and departments including asset management planning, activity planning, contract management, legislative compliance, occupational health and safety, human resources, professional advice; security, financial management, reputational exposure, management reporting, records management, information technology, and systems;
- the liability risk assessments undertaken by Councils public liability insurer;
- legislative, regulatory and /or industry information obtained from various sources;
- feedback received from the communication and consultation process both from external and internal stakeholders;
- employees and members of the public are also encouraged to report potential risk exposures.

Each risk identified will be entered and maintained in the risk register.

Step 3: Risk Assessment

Risk analysis aims at understanding the level of significance of a risk and ways to control and/or mitigate it.

A full accurate and objective assessment of any identified risk must be undertaken to:

- determine existing controls;
- determine the risk likelihood;
- determine the consequence of the risk;
- establish the risk rating.

An assessment of risk should be carried out three times during the life of the risk:

- Stage 1:
  Inherent risk - the risk exposure prior to management controls being put in place;
- Stage 2:
  Managed risk – the risk exposure with the current level of management controls;
- Stage 3:
  Residual risk – when no further controls are required and the level of risk is tolerable.

Step 4: Risk evaluation

After the likelihood and consequence factors have been determined, the level of risk is calculated by multiplying the Probability/Likelihood of the risk occurring with the Consequence or Impact Levels. The final outcome is the risk rating.

The results of the risk evaluation will determine in the first instance the risk management strategies that will be required to be tailored to the risk profile. Once the risk has been assessed according to the relative risk level it poses, it is then possible to target the treatment of the risk exposure.

Step 5: Risk Treatment

The treatment of risk is dependent on a number of factors including Councils risk appetite and selection of risk control options.

Risk control options include:

- **Risk avoidance** – avoid the identified risk by deciding not to proceed with the activity likely to generate risk (where this is practicable);
- **Risk transfer** – reducing exposure by transferring the risk to another party e.g. contracting out;
- **Reduce the likelihood** of occurrence through measures such as audit compliance, programmes, contract conditions, preventative maintenance, engineering controls, inspections, process policies and procedures; and
- **Reduce the consequence** through measures such as contingency planning, disaster recovery plans, contractual arrangements, financial management controls and risk minimisation plans.

Residual risk

Residual risk is the risk left after the risk treatment process has been performed and controls applied. The acceptance of residual risk is dependent on Council's agreed risk appetite and cost-benefit analysis of options.

Monitoring and review

Risks are constantly changing so risk needs to be systematically and periodically monitored and reviewed.

4.2 Key principles in risk management

The following key principles outline the Council's general approach to risk management:

(a) The identification and management of risk is linked to the achievement of the Council's strategic goals and responsibilities;

(b) The Council, through its Finance, Risk and Audit Committee is responsible for overseeing a sound system of internal control that supports the achievement of its operations;

(c) The Council makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks;

(d) Review procedures cover reputational, strategic, operational, compliance and financial risk;

(e) Risk assessment and internal control are embedded in on-going operations, business as usual;

(f) The CEO and Senior Leadership Team are responsible for encouraging and implementing good risk management practice; and,

(g) The Finance, Risk and Audit Committee will receive reports at each meeting on internal control and risk identification, evaluation and mitigation review.

4.3 Specific principles

WDC's attitude and approach to risk has been informed by the eleven risk principles contained in *ISO3100: 2009 Risk Management*, and can be articulated through the following risk management principles:

(a) WDC intends to comply with all applicable laws, regulations and policies;

(b) WDC employees will model behaviours that are consistent with our values, good practice, and relevant policies;

(c) Risk is inherent in all endeavours. Taking calculated risks is fundamental to organisational planning and decision making and the successful achievement of objectives;

(d) Risk taking that is uninformed and/or outside of WDC's defined risk appetite will not be tolerated;

(e) All employees of WDC are the owners of the risks and obligations arising from within their areas of operations or as a result of their actions; and,

(f) All employees have an obligation to appropriately report any issues, risks, compliance breaches or exceptions that they encounter.

4.4 Objectives

In the context of these principles, the objectives of the Risk Management Policy are to:

(a) Provide a simple method and balanced approach for all staff to minimise exposure, loss and damage whilst realising opportunity and delivering improvement;

(b) Integrate risk management with governance and management arrangements, embedded in major organisational and business processes, and to clearly specify its accountability; and,

(c) Align the Council's risk management approach with the *ISO 31000 Risk Management Standard* and provide a consistent language in the consideration of risk across all Council activities.

4.5 Risk appetite

The risk management strategies developed and acceptable residual risk are required to take into account Council's agreed risk appetite.

The appetite is reviewed and updated on an annual basis following the consideration of a range of factors including organisation and Council views, strategies and the internal and external risk environment. Once implemented, the appetite is used to drive decision making about risk.

The WDC risk matrix in Appendix 1, which covers a number of critical risk categories, serves as a statement to the Council's appetite and the boundaries of acceptable risk taking. Responsibility to define the risk appetite rests with the Council through the Finance, Risk and Audit Committee and will be done by approval of this framework on an annual basis.

4.6 Statutory framework

Though there is no explicit requirement for local authorities to have in place a risk management framework, numerous legislative requirements talk to the demonstration of risk management elements. By providing a whole-of-Council approach to managing risk, based on the *ISO31000: 2009 Risk Management Standard*, this policy gives WDC a method to demonstrate appropriate risk management arrangements, now and into the future.

5. Roles

5.1 Elected members

Council will:
(a) ensure an appropriate risk governance structure is in place;
(b) support Corporate Risk Management Framework including risk management as an element of the Councils' Long Term Plan and Annual Plans as well as other strategies, plans and documents;
(c) be responsible for setting risk appetite.

Finance, Audit & Risk Committee will deliver on its mandate as outlined in its delegations including acting in a risk monitoring advisory and improver role for Council. The Audit and Risk Committee should support the overall risk management process by:

(a) ensuring Council has appropriate risk management and internal controls in place;
(b) approving and review risk management programmes and risk treatment options for extreme risks;
(c) being responsible for making recommendations to Council for setting risk appetite;
(d) providing guidance and governance to support significant and/or high profile elements of the risk management spectrum.

5.2 Role of management

Senior management must familiarise themselves with this policy so that they can:

(a) Understand and implement the policy on risk management within their respective areas of responsibility;

(b) Ensure compliance with risk assessment procedures such as the Internal and External Audit Programme; and,

(c) Embed risk management activities as part of the system of internal control.

5.3 Three lines of defence

WDC has adopted a 'three lines of defence' approach to governance assurance as illustrated below

First line of defence; Council staff	***Responsibilities***
Risks reported to line managers	All staff including management, team leaders and General Managers are required to: • Apply the risk management framework day-to-day. • Identify, manage and report risks, issues and incidents that may impact on operational, project and strategic objectives. • Take ownership and demonstrate accountability for risk. • Actively promote a positive risk culture. • Participate in risk training and awareness requirements and improvement activities.
Second line of defence; senior management	***Responsibilities***
Risks reported to the Chief Executive and the senior management team	• Oversight and integration of risk management activities conducted by the first line of defence into business activities. • Conduct activities to develop risk culture. • Design risk management frameworks and methodologies. • Ensure risk owners manage their risks. • Undertake risk reviews and monitor risk management control procedures and performance against risk appetite. • Manage the risk registers and reports.
Third line of defence; internal audit	***Responsibilities***
Risks reported to the Finance, Risk and Audit Committee	• Provide independent assurance and oversight for first and second line defence. • Provide assurance to the Council, via the Committee of the design and operating effectiveness of systems and internal controls in order for the Council to discharge its

governance responsibilities.

5.4 Business as usual procedures

Business as usual procedures encompass a number of elements that together facilitate an effective and efficient operation, enabling WDC to respond to a variety of risks. These elements include:

(a) Environmental scans (keeping ourselves updated on our operating environment);

(b) The Integrated Reporting Framework for the Council and the Senior Leadership Team tracking progress towards the achievement of the strategic goals;

(c) Department planning and budgeting – the department planning and budgeting process is used to set actions and allocate resources. Progress towards meeting plan targets is monitored regularly;

(d) Major projects (risk assessment and mitigation strategies are essential elements);

(e) High-level Risk Register – to identify, assess, and monitor risks significant to the Council. The risk register is revised four times a year and emerging risks are added as required; and,

(f) Assurance measures (internal audit, reporting).

5.5 Internal audit programme

The internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation. The internal audit strategy is developed around the Council's goals and responsibilities.

5.6 Third party audits

External audits will be conducted in line with the Council's established audit procedures and legislative requirements.

6. Types of risk

All risks must be identified and managed, however due to limited resources; a prioritised approach has been adopted. Only key risks or material risks that will impact WDC's strategic and business objectives are recorded in the WDC strategic risk register and administered by the Finance, Risk and Audit Committee. There are currently operational and tactical risk registers and risk management in place, these are maintained and overseen by the relevant member of the Senior Leadership Team.

To ensure there is practical approach to identifying, managing and reporting risks, it is useful to understand that risk cascades through each level of the organisation and is inherent in all of WDC's activities, systems and processes. Risk generally falls into three broad types:

(a) **Strategic risks** - generally emanate from WDC's strategic activities, systems and processes and would impact or impede achievement of WDC's strategies.

- Captured through key planning documents, e.g., long-term plans, annual plans, asset management plans and financial strategy and reported through governance reports.

(b) **Tactical risks** - generally emanate from key project activities, systems and processes and would impact or impede achievement of project objectives.

- Captured and reported through project briefs and plans.

(c) **Operational risks** - generally emanate from business unit and team activities, systems and processes and would impact achievement of specific business unit objectives.

- Captured and reported through business planning process.

Each risk owner remains responsible for managing all assigned risks whether they are recorded and managed in the Council's register or independently.

All risks that fall within the Council's risk reporting criteria or when a significant change in a risk that would cause it to breach the Council's risk appetite must be reported to the Chief Executive.

To ensure there is a dynamic iterative approach to risk management, the Finance, Risk and Audit Committee will conduct regular risk reviews.

Operational	
Potential losses or adverse impacts resulting from inadequate or failed internal processes, people and systems or from external events, excluding strategic risks.	• Occupational health & safety (there is a separate risk register for this area) • HR/people • Fraud • Information technology • Accounting/finance • Project management • Legal & compliance • Outsourcing & procurement • Business operations & practices • Business continuity • Environmental compliance
Asset	
The potential of financial loss or adverse impacts arising from WDC's assets.	• Capacity • Liability risk • Capital investment • Renewal Risk • Level and continuity of service • Property damage • RMA compliance
Financial	
The potential for loss or adverse impacts resulting from WDC's finance activities.	• Insurance management • Financial strategy • Debt risk • Financial sustainability • Treasury
Council	
The potential for loss or adverse impacts arising from poorly designed and implemented strategies, business decisions or improper implementation of those business decisions, unforeseen events beyond the Council's	• Tactical • Governance • Catastrophic • Strategic

control, lack of or ineffective planning, lack of responsiveness to change, ineffective governance, external factors and changes.	• External • Reputational • Emerging • Environmental compliance

7. Legislative compliance

The Council is bound by a wide range of legislation that sets out its powers, duties and responsibilities. Compliance with this legislation is a responsibility that is shared between the staff and the elected members. Oversight will be maintained by the Finance, Risk and Audit Committee reporting to the full Council.

8. References

ISO31000: 2009 Risk Management Standard

APPENDIX 1: PROBABILITY/LIKELIHOOD LEVELS

1 Likely	• **The event will probably occur in most circumstances; or,** • **Not quarterly but within 6 months.** • **70% chance of occurring in the next 12 months.**
2 Moderate	• **The event will possibly occur at some time; or,** • **Not within 6 months but at least annually.** • **50% chance of occurring in the next 12 months.**
3 Rare	• **The event could occur at some time; or,** • **Not annually but within 3 years.** • **20-30% chance of occurring in the next 12 months.**
4 Very rare	• **The event may occur only in exceptional circumstances; or,** • **Not every 3 years but at least every 10 years.** • **10-20% chance of occurring in the next 12 months.**
5 Unanticipated	• **The event is not expected to occur; or,** • **Not within 10 years.** • **2% chance of occurring in the next 12 months.**

APPENDIX 2: CONSEQUENCE LEVELS

LEVEL	DESCRIPTOR	CATEGORIES						
		Health & Safety	**Environmental Contamination**	**Statutory Obligations**	**Image & reputation**	**Loss of Service**	**Project Delay**	**Financial Loss**
1	**In-significant**	No injury or potential minor injury	No contamination	Internal query	Customer complaint	Unable to operate for less than 1 day	Less than 6 months	<$5,000; Council <$50,000 Community
2	**Minor**	Minor injury	On-site release immediately contained	Special Audit by outside agency or enquiry by Ombudsman	Negative community coverage	Unable to operate for 1 day – 3 days	Between 6 month and a year	<$10,000; Council <$100,000 Community
3	**Moderate**	Risk of injury (Some severe injuries or potential injuries (near miss))	On-site release contained with outside assistance	Litigation	Negative community and some regional coverage	Unable to operate for up to a fortnight	Between 1 – 3years	<$100,000 Council; <$500,000 Community
4	**Major**	Actual injury or risk of serious injury (Significant illness or some deaths (up to 3))	Off-site release with significant detrimental effects	District or Environmental Court	Negative regional and some national media coverage	Unable to operate for up to 1 month	Between 3 – 5 years	<$500,000 Council; <$1,000,000 Community
5	**Catastrophic**	Serious injury and death (Wide-spread illness or several deaths (>3))	Toxic release off-site with major detrimental effect	High Court or Criminal Action	Sustained negative national media coverage	Unable to operate for >1 month	More that 5 years	>$1,000,000 Council; >$5,000,000 Community

APPENDIX 3: LEVELS OF RISK

Comparative Levels of Risk		
E	Extreme Risk	Immediate action required to manage risk - reported to Council
H	High Risk	Senior management attention to manage risk - reported to FARC
M	Considerable Risk	Management responsibility must be specified and risk controls reviewed
L	Low Risk	Managed by routine procedures

APPENDIX 4: RISK MATRIX

Probability/ Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likely	M	H	E	E	E
Moderate	M	H	H	E	E
Rare	L	M	H	E	E
Very Rare	L	L	M	H	E
Unanticipated	L	L	M	H	E

Appendix 5: Managing and reporting risks

Criteria for Management of Risk	Rating and Monitoring
• Risk Acceptance: Council • Risk Ownership: Finance, Audit and Risk Committee	At least monthly **Extreme**
• High risks can exceed risk appetite and tolerance limits. • High risks within WDC's control must, where feasible, have effective key controls. • Immediate escalation to the Council is required. • Immediate action is required.	
• Risk Acceptance: Finance, Audit and Risk Committee • Risk Ownership: SLT	At least every 2 months **High**
• High risks usually exceed risk appetite and tolerance limits. • All High risks must, where feasible, have effective key controls. • Immediate escalation to SLT member. • Action begins within 1 day.	
• Risk Acceptance: SLT • Risk Ownership: Tier 3 managers	At least quarterly **Considerable**
• Considerable risks may exceed risk appetite and tolerance thresholds. • Considerable risks must have controls. • Escalate within 2 days to Tier 3 manager. • Action begins within 1 week.	
• Risk Acceptance: Tier 3 manager • Risk Ownership: Relevant officer	At least annually **Low**
• Low risks are usually within risk appetite and tolerance limits. • Low risks should have adequate controls in place. • Escalate within 1 week to Relevant Manager • Action by standard operating procedures	