greater WELLINGTON
REGIONAL COUNCIL

Risk Management Policy

This policy sets out the responsibilities for and the process of risk management

Policy owner	Chief Financial Officer
Position administering this policy	Treasurer
Date policy comes into effect	The first working day following the date of approval by the Chief Executive.
Related policies	Risk Management procedures Project Management policy Being Safer together – Health & Safety Management System
Policy establish date	By September 2013
Policy history	This policy was reviewed in 2016.

Approved: Greg Campbell Date: May 2016

Chief Executive

POLP – 50845999-236

Contents

1. Background

Formal Risk management identification recording and reporting began with the introduction of Quantate Risk & Assurance database in 2009. This risk management policy and associated risk management procedures were updated in May 2016.

2. Scope

This policy covers all groups of Greater Wellington and its subsidiary companies excluding CentrePort Limited.

3. Definitions

Risk - is the effect of uncertainty on Council's ability to achieve its objectives.

Risk appetite - is the amount and type of risk that the Council is prepared to accept in the pursuit of its objectives.

Risk management process - is the systematic application of management policies, processes and practices to activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risks.

Risk assessment - the overall process of risk identification, risk analysis and risk evaluation.

Risk register – is the record of information about identified risks and how they are being managed. The Council has adopted Quantate as its risk register which is a data base used to record, evaluate and report the Council's risks.

Control - a measure that modifies a risk and may include any process, policy, practice or action. Generally, controls are designed to reduce risk, but may also change how the consequences are felt.

Likelihood - the chance of the risk eventuating. This may be expressed as the possibility of an event giving rise to the consequences.

Consequences - these are the impacts or events which may be quantitative (e.g. monetary impact) or qualitatively (i.e. impact on perception) or quality of output.

Inherent risk - is the raw state, or before any controls are applied to modify or reduce the risk.

Residual risk – is the risk that remains after any controls are applied to modify that risk.

Risk treatment or risk treatment option - a control that is currently being considered, i.e. an option designed to modify a risk source by removing the risk source or, changing the likelihood, or altering the consequences.

4. Council's risk management objectives

The main objectives of this policy and risk management when implemented are to:

- increase the likelihood of the Council achieving its strategic and business objectives
- safeguarding, the Council's assets and those people using them, people resources, finances and reputation
- ensure risk management practices are integrated into all Council operations and processes
- provide a timely response to risks escalation and issues as they occur
- promote awareness of risk management process and a culture of risk management awareness such that *everyone in the organisation is responsible for managing risk*
- aid decision making
- maintain a flexible and evolving risk management framework which is aligned with AS/NZS 31000:2009 and best practice generally.

5. Principles of risk management

For risk management to be effective at all levels within the organisation Council endeavours to comply with the following principles (underlying concepts and drivers), with *risk management:*

- creating and protecting value
- is an integral part of Council processes
- is part of decision making
- explicitly addresses uncertainty
- is systematic, structured and timely
- is based on best available information
- is tailored
- takes into account human factors
- is transparent and inclusive
- is dynamic, iterative and responsive to change
- is capable of continual improvement and enhancement

Source:- AS/NZS ISO 31000:2009

6. Organisational roles and accountabilities

The Council's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well defined roles and responsibilities.

The Council's risk management policy is applicable to all Council staff. It is of importance that each individual staff member is aware of their collective risk management responsibilities.

The Council requires that appropriate risk management is in place and that they are made aware of risks that may impact on the delivery of the organisation's plans.

The *Finance, Risk and Assurance Committee* (FRA) under its terms of reference monitors the identification and management of risks faced by Council, including any assurances sought or initiated by management and other relevant authorities (notably auditors) on the efficacy of risk management policies and practices.

The *Internal Audit* function provides the executive with assurance based on independence and objectivity that risk management is being undertaken and implemented in accordance with this policy.

The *Chief Executive* (CE) has overall responsibility for ensuring the organisation has a risk management framework in place that identifies risks, monitors and manages risk and ensures the Council is aware of material risks facing the organisation. The CE approves this policy for implementation.

The *General Manager* for each of the organisation's groups is responsible for ensuring that risks are identified in their area, that they are monitored, controlled and reported on. Promotes risk management awareness culture in day to day activities.

The *Chief Financial Officer* is the reporting officer to the FRA Committee and is responsible for ensuring appropriate recording, reporting and risk management processes are in place.

The *Treasurer* is the risk management coordinator, and responsible for the organisations risk register. The Treasurer liaises with the groups business managers and ensures the risk management processes around the register are undertaken.

The *Business Manager* in each group is responsible for the group's risk management. The Business Manager coordinates regular meetings on risk management and has the responsibility for reporting and liaison with the risk owners and for the recording of risk data in the risk register.

The *Risk Owners* have the ultimate ownership of individual risk recorded and reported in the risk register. Each risk has an assigned risk owner.

The *Project Owners* who supervise and run projects are responsible to ensure that project risks are documented as part of their project management and added to the organisations risk register. Project management risk process is currently under review and will provide a framework that links to the Quantate risk register.

The *Control owners* have the ultimate ownership of the individual controls which modify risks. In many cases they are the risk owners as well.

The *Control Assessor* is the person assigned to assess that the control is working as reported. The Control Assessor is appointed by the Control owner in consultation with the Business Manager.

7. Risk management process

A risk management framework is the overarching process that provides the foundation and organisational arrangements for identifying, designing, implementing, monitoring, reviewing, reporting and continually improving the management of risk for the organisation.

The risk management process is shown below and each section discussed in turn.

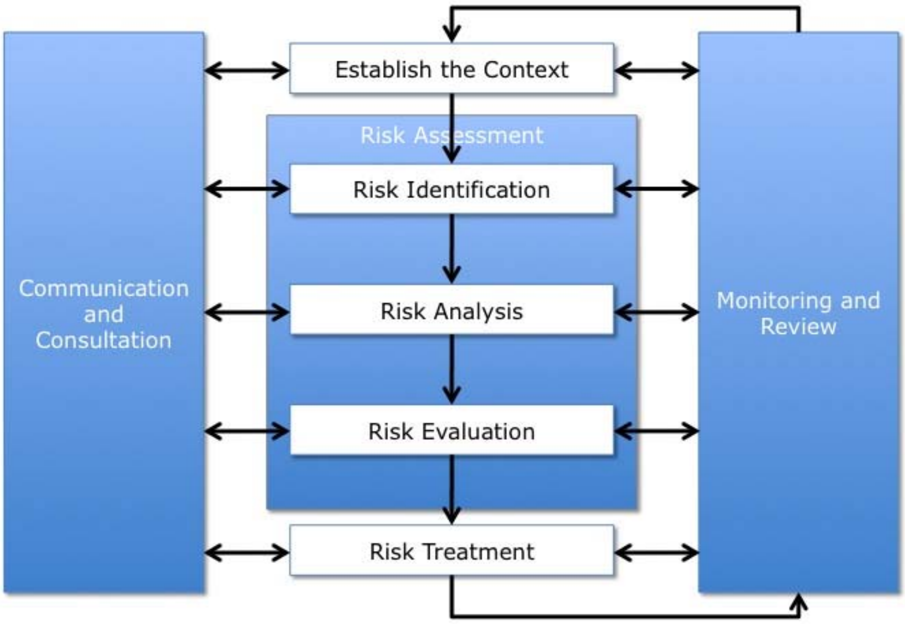

Figure 1- ISO 31000 Risk Management Process

7.1 Establish the Context

Establishing the context for the Council's risk management process is a key step because it builds an understanding of the Council's internal and external stakeholders. The external context is the extent to which the Council's external environment will impact on the Council's ability to achieve its corporate objectives. The internal context is about understanding the internal operating environment and the way its components interact – people, culture, goals and objectives.

Establishing the risk management context takes into account the Council's goals, objectives, strategies, and scope, and sets the parameters of the risk management process in line with the risk appetite set by the Finance, Risk and Assurance Committee in conjunction with management. The inputs to the Council's risk appetite are shown as in figure 2 below:

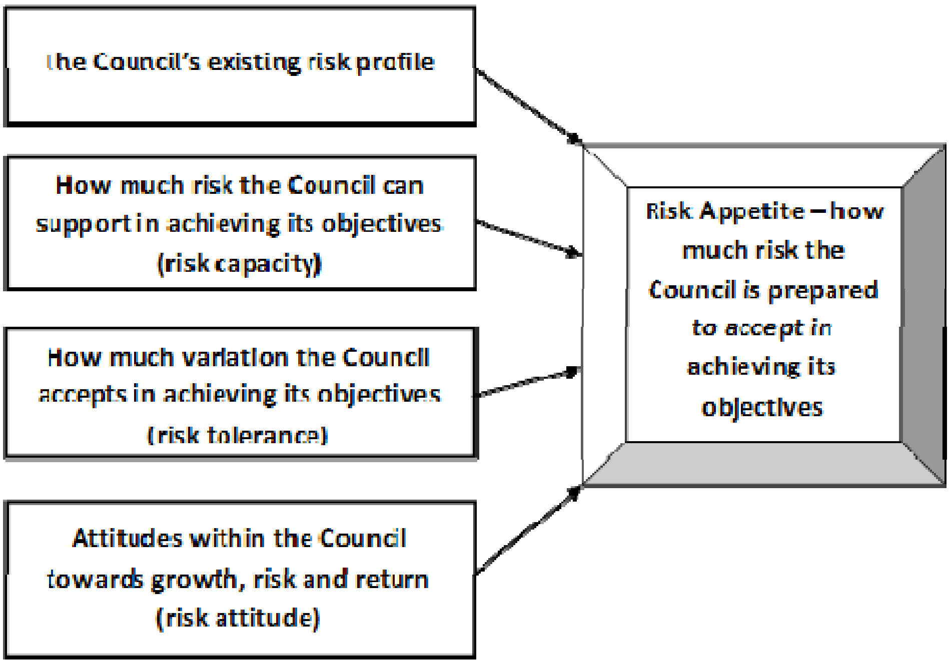

Figure 2 - Considerations that determine the Council's risk appetite

Council generally has an averse to balanced risk appetite. The Council's lowest risk appetite relates to, health and safety, legislative and regulatory compliance, and environmental damage, with a marginally higher risk appetite towards other risk categories. This is further discussed under figure 3.

8. Risk assessment including, risk identification, risk analysis, and risk evaluation

8.1 Risk identification

Comprehensive risk identification is crucial to the overall effectiveness of risk management.

The identified risks will determine the 'what', 'why', and 'how' things can happen as a basis for further analysis. There are many sources of risk the Council is exposed to and they are categorised, see figure 3, which also includes the Councils risk appetite for each source. Appendix 2 expands on the sources of risk.

Source of risk	Risk appetite*		
	Averse	Balanced	Tolerant
Loss, failure or damage to assets		X	
Services being severely curtailed		X	
Health & safety to staff and contractors	X		
Financial, macroeconomic risk		X	
Subsidiary companies and Trusts		X	
Legislative and regulatory	X		
Political		X	
Projects		X	
Environmental damage	X		
Human Resources		X	

Figure 3 –Sources of risk – incorporating risk appetite

* Averse means being unwilling to take on anything other than small risks. Balanced means having an appetite between averse and tolerant (i.e. a flexible approach). Tolerant means being willing to take on significant risks to exploit opportunities despite potentially major consequences if the risk is realised.

Risk analysis and risk evaluation

Risk analysis and risk evaluation are undertaken utilising the Quantate risk and assurance management software. Quantate's approach to risk management is summarised below.

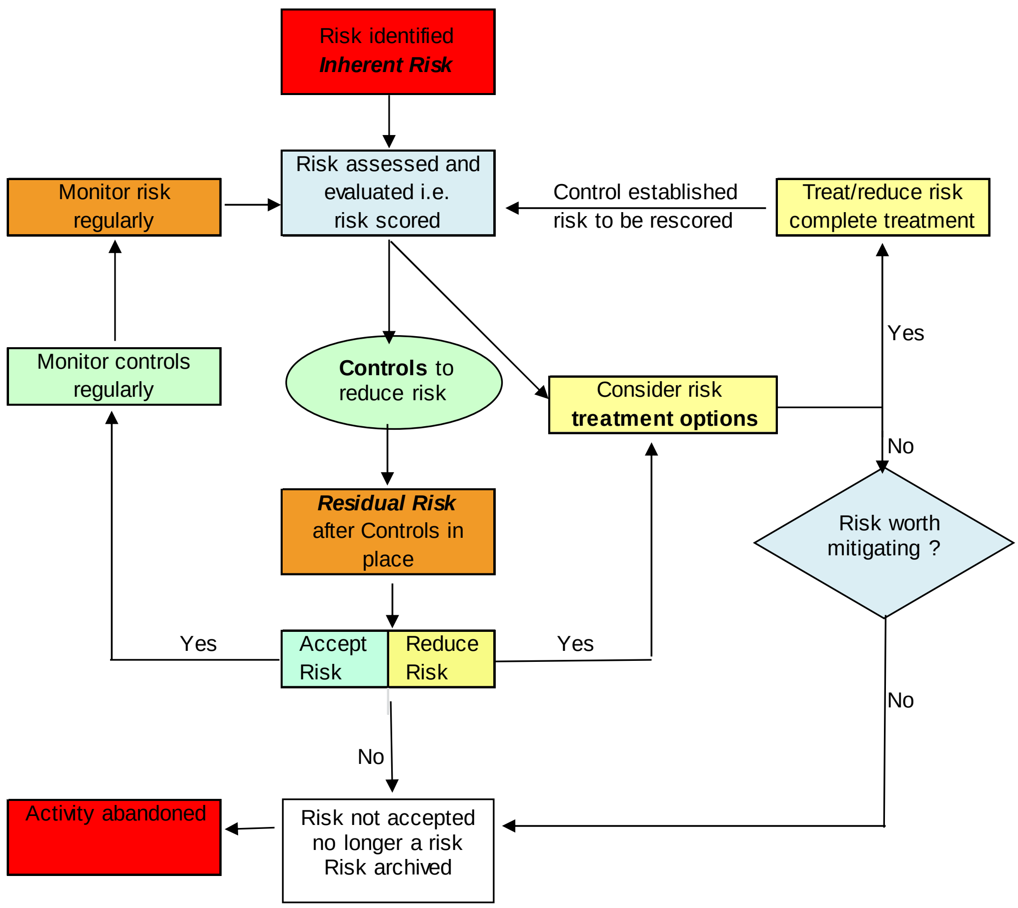

Figure 4 – Quantate Risk Overview

A risk, identified in its untreated state is known as an *inherent risk*, once it has been assessed and controls identified to reduce the risk, it is known as a *residual risk*.

A *risk treatment option* is a control being considered for implementation. Once a treatment is accepted and in operation it becomes a *control*.

Under the Quantate risk management system, each recorded risk has an owner, and each recorded control modifying that risk has an owner.

One way of assessing risk is to look at the various levels of the organisation where risks are identified and how they are controlled and reported on.

Risk Management Framework by risk type

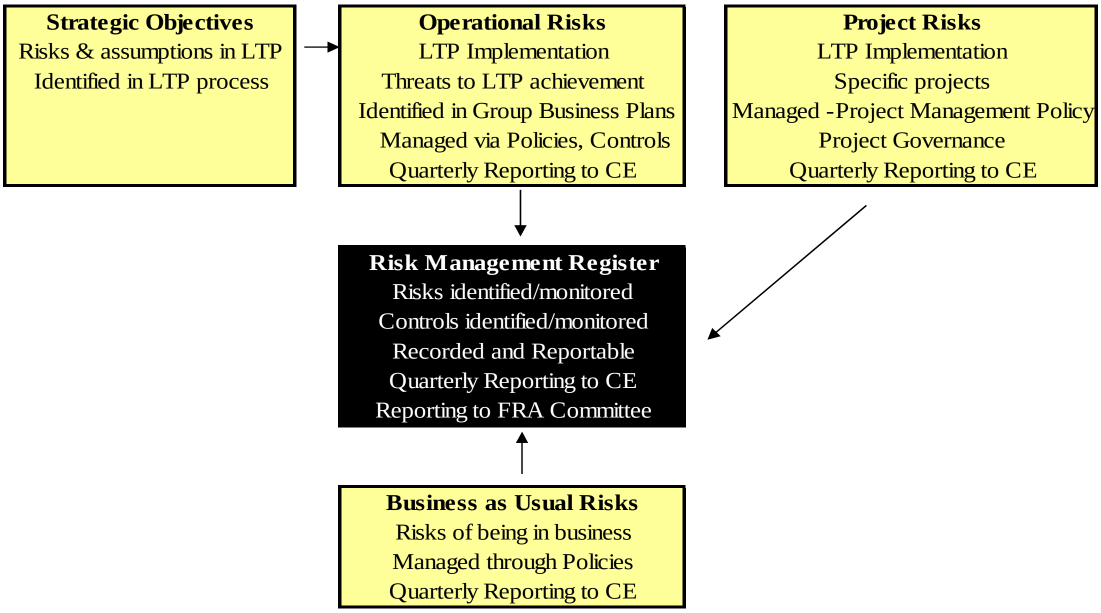

Figure 5 – Risk Management Framework by risk type

8.2 Risk analysis

The purpose of the risk analysis step is to define the significance of a risk by assessing its consequence and likelihood of occurrence (also known as risk criteria), taking into account the processes and controls to mitigate it.

The risk criteria used to analyse a risk i.e. consequence and likelihood, are included in Appendix 1.

Inherent risk is the risk that exists if there were no controls, or if the controls all failed to work while *residual risk* is risk left over after the risk has been treated e.g. through the use of *controls.*

Therefore, there is a need to analyse risk before and after the application of controls, which are intended to reduce risk to an acceptable level (i.e. within the Council’s risk appetite). This approach to analysing the risks allows the assessment of whether existing controls are enough to manage the risks or whether additional controls i.e. *risk treatments* are needed.

Quantate has a systematic approach to establishing, recording and monitoring controls. There are two types of controls available, *generic controls* which are controls that have been set up in the system and can be used by anyone, and *risk specific controls*. Risk specific controls are specifically tailored to a specific risk.

Controls vary in level of importance depending upon their criticality or ability to reduce the consequences or likelihood of the risks impact.

Each control has an assigned owner. The control could be a plan, a policy, or a specific process implemented to modify a risk.

8.3 Risk evaluation

Once the consequences and the likelihood are chosen the risk management software weights them mathematically to determine a risk score.

The score of a risk is a function of its consequences and the likelihood of occurrence of those consequences. The consequence of a risk is measured across the dimensions of operational, financial, health & safety, environmental and stakeholder/reputational impacts.

The result of calculating the likelihood and the consequences scores the *inherent risk*. When the effects of the controls are included the result is a reduction in either or both the likelihood of occurrence or consequence of occurrence which results in a *residual risk*.

The resultant output from the risk management software after the risk criteria are scored is a ranking which falls within the following categories. These categories are derived from a chart that has predetermined levels which determine the risk scoring. See figure 5. In this example the IR – *Inherent risk* is untreated risk at the top the Chart and the RR – *Residual risk* after controls are implemented is at the middle of the chart.

Level of Risk	Very High Risk	High Risk	Medium Risk	Low Risk

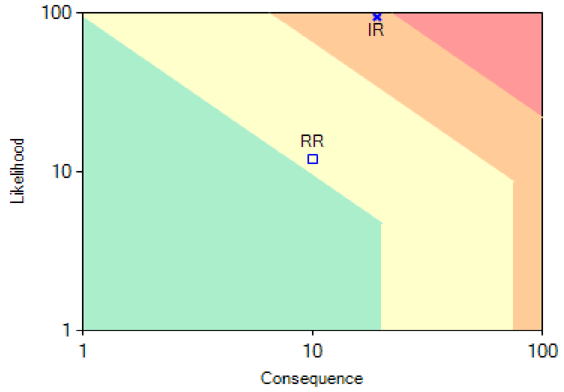

Figure 6 – Risk scoring levels

The likelihood/consequence chart recognises the level of risk is not linear, for example a low likelihood of occurrence with a high consequence impact still produces a high risk score. Depending upon where the residual risk lands on this chart determines how it is dealt with as discussed below.

Very High Risk:

Inherent Risks - Risks without controls should be treated immediately

Residual Risk - Further treatment should be considered immediately. Only tolerable if the cost of risk treatment far outweighs the benefits. If the level of opportunity presented is not significant, consider ceasing operations that creates this risk exposure or a revised strategy to increase the opportunity.

Requires review by the applicable General Manager, Chief Executive and is to be brought to the attention and Finance Risk and Assurance Committee for review quarterly.

High Risk:

Inherent Risks - Risks without controls should be treated immediately

Residual Risk - Further risk treatment should be considered. The level of risk is acceptable if the cost of treatment outweighs the benefits that the treatment would deliver. Requires the Chief Executive and the applicable General Manager to review at least quarterly.

Medium Risk:

Inherent or Residual Risk - Risk is acceptable, provided that the risk is managed as low as reasonably practicable. Requires operational attention with quarterly review by the applicable General Manager.

Low Risk:

Inherent or Residual Risk - Risk is generally acceptable and consideration of treatment is only warranted if cost of treatment is low with tangible, certain benefits. Requires operational attention with bi-annual review by the applicable General Manager and/or the Business Manager.

9. Risk treatment

Risk treatment involves determining the appropriate options for managing the risks identified.

Treatment options are required where the current controls are not mitigating the risk within defined tolerance levels as determined by the first step (establishing the context).

Treatment options might include one or more of the following:

- *Avoid or eliminate* the risk by not proceeding with the activity likely to trigger the risk. Risk avoidance must be balanced with the potential risk of missed opportunities.
- *Accept* the risk.
- *Reduce* the risk by reducing the consequence and/or likelihood of it occurring.
- *Transfer/share* the risk in part or entirely to others (e.g. through insurance or a third party).

When determining the preferred treatment option consideration should be given to factors such as cost or reputation (e.g. a cost/benefit analysis). The treatment should be monitored and reported to the general manager on how the implementation of the action is progressing.

Risks that remain outside the Council’s risk appetite after this point will be escalated to the chief executive and the Finance Risk and Assurance Committee.

10. Communication and consultation

The communication process is for both the external and internal stakeholders.

For external stakeholders this means:

- Informing them of the Council's approach to risk management and its effectiveness

- Gathering their feedback where necessary to improve the Council's risk management process. Much of this is undertaken during the annual plan and long term planning process or through open consultation and community involvement.

For internal stakeholders this means:

- Communicating to them the Council's risk management process and their roles and responsibilities in it

- Ensuring accountability for fulfilling those roles and responsibilities in relation to the process

- Seeking feedback about the effectiveness of the process

11. Monitoring and review

Risk Reporting

Each group within the organisation has an appointed business manager whose function is to coordinate the reporting from the risk register.

Each group is to report their risks in an organisation wide approved format which is determined by the chief financial officer in consultation with the chief executive from time to time.

The format will list a description of the risk, its risk score, the controls, who is responsible for the risk and any changes to the risk or items of interest relating to the risk over the last quarter.

Each quarter, or as determined by the Council timetable, the Finance Risk and Assurance Committee will receive a report on the organisation's risk management.

This report will bring to the attention of the Committee any risks that have been identified by the chief executive/chief financial officer as warranting particular mention.

The reporting will focus on changes to the risk register over the quarter, this will include new risks added to the register, risks archived from the register and any changes in scoring. Other items recorded might include emerging risks, or other items management wishes to bring to the Committee's attention.

As well as the above each quarter a group within the organisation will present to the Committee on their risks and their current risk management activities. This provides the Committee over the period of a year with a comprehensive listing and discussion on the Councils risks.

Risk and process review

Good management of risk requires continued review and process improvement.

The following review is to be undertaken according to the time frames indicated.

- *Risk Criteria* are to be reviewed at least every five years or after any significant organisational change or event to ensure they reflect the best fit for the organisation.

- *All risks* are to be reviewed at least quarterly. This includes reviewing the groups business and considering any new risks that may have come about.

- *All controls* are to be monitored on a regular basis to ensure their confidence and reliability. The frequency of monitoring is assessed by the business manager and recorded in the risk register. The criticality of a control will determine how often it is assessed and is prompted for the business manager by the Quantate risk register with suggested frequencies.

- *The Risk Management Policy* is to be reviewed every three years to ensure it reflects best practice in terms of this organisation, with the next review to occur in 2019.

- *The Risk Management Procedure* – on Council‘s intranet Gwennie under Job Tools & Guides/Finance and procurement guides/ Risk Management/ sets out the quarterly risk review process. To be reviewed at the same time as the Risk Management Policy.

The Three Lines of Defence - Effective Risk Management & Control

Are we managing risk properly? The three lines of defence is a model that provides a clear and effective way to strengthen communication on risk management, assurance, and control by clarifying essential roles and duties for various parts of governance, management and day to day operations.

- **The first line of defence –** ***operational risk and control in the business***

  Operational managers own and manage risks and are responsible for implementing corrective action to address control deficiencies. They are responsible for identifying controls, maintaining effective controls, assessing controls and mitigating risk. Operational managers are the *Business Manager, Risk Owners, Project Owners, Control Owners and Control Assessors.*

- **The second line of defence – *the oversight functions***

  The responsibility of the second line functions is typically reviewing risk management reports, checking compliance with the risk management framework, and ensuring that the risks are actively and appropriately managed. This includes drafting policy, aligning strategy, setting direction, introducing best practice, and providing oversight and assurance to the Council. The second line function includes *the Treasurer, Chief Financial Officer, General Managers and the Chief Executive.*

- **The third line of defence – *independent assurance providers***

  This is the role of internal audit to provide independent, objective assurance and feedback designed to add value and improve the risk management process. The Finance Risk and Assurance Committee's role in this is to maintain oversight and to monitor the effectiveness of the risk management process as well as the abovementioned audit activities. The third line function includes *Internal Audit, External Audit and the Finance Risk and Assurance Committee.*

Appendix 1- Risk criteria

Risk Criteria:
Consequences - Operational Capability

Assessment Level	Full Description	Value
Level 5 Diversion >12 months	Event results in management diversion from strategic objectives for a period of > 12 months and/or delivery of LTP outcomes across work area significantly affected for greater than six months. Critically detrimental effects on stakeholders. Long term loss of capability (>12 months) and/or severe staff morale problems may likely arise leading to loss of a significant number of key senior staff, impacting on skills, knowledge and expertise.	85
Level 4 Diversion >6 months	Event results in management diversion from strategic objectives for a period of > 6 months and/or delivery of LTP outcomes across work area significantly affected for up to six months. Moderate detrimental effects on stakeholders. Event results in loss of operational capability for up to 2 months and/or major morale or other organisational problems affecting performance and productivity may arise and could lead to loss of key staff within two or more areas of council, resulting in skills, knowledge and expertise deficits.	35
Level 3 Diversion >2 months	Event results in management diversion from strategic objectives for a period > 2 months and/or delivery of LTP outcomes across work area significantly affected for up to one month. Minor detrimental effects on stakeholders and/or major morale or other organisational problems affecting performance and productivity may arise and could lead to loss of key staff skills, within one area of council, resulting in skills, knowledge and expertise deficits within this area of council.	12
Level 2 Managed	Event reduces efficiency or effectiveness of service. Managed internally with no or limited diversion from strategic objectives and/or Moderate staff morale problems resulting in some staff resignations but managed through minor restructuring.	7
Level 1 Minor	Event causes minor disruption felt by limited small group of stakeholders and/or Minor staff morale impact resulting in minor dissention but managed over a short period of time.	3
No impact	No impact on operational capability	0

Consequences - Stakeholders /Reputation

Note: '**Stakeholder' means** clients, public, industry groups (such as forestry/agriculture), local government bodies, lobby groups, or Iwi.

Assessment level	Full Description	Value
Level 5 Extreme	Extreme dissatisfaction and loss of confidence by stakeholders and/or regulatory body investigation and/or statutory management installed and/or significant sanctions against the organisation. Regulatory action resulting in major prosecution and conviction of council (e.g. fine of >$100k).	95
Level 4 Major	Major loss of stakeholder confidence and/or extensive stakeholder dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months). Widespread, unified, coordinated revolt by consent holders and/or ratepayers against fees/conditions or sanctions imposed against the organisation. Regulatory action resulting in moderate prosecution and conviction of council (e.g. $25-$100k)	45
Level 3 Moderate	2-3 stakeholders sectors dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months) and/or Central Government impose statutory sanctions. Regulatory action resulting in prosecution but no conviction.	15
Level 2 Single	Single stakeholder sector express dissatisfaction through national media for up to one month and/or Central Government – CEO, Ministry for the Environment directed by Minister to make enquiries and/or Regulatory action resulting in investigation but no prosecution	7
Level 1 Individual	Individual(s) express dissatisfaction through local media to GWRC directly and/or Individual(s) refuse to pay fees/rates as a stand against council activities and/or Breach of law with internal investigation with minor changes to operations.	3
No Impact	No significant impact on stakeholders or image	0

Consequences - Health and Safety

Assessment level	Full Description	Value
Level 5 Extreme	Extremely harmful - Multiple fatalities	85
Level 4 Major	Very harmful - Single fatality and /or multiple severe injuries/disabilities	35
Level 3 Significant	Harmful - Serious injury and/or permanent disability. Lost time injury > 1 week	12
Level 2 Moderate	Slightly harmful – Medical aid required. Lost time injury < 1 week	7
Level 1 Minor	No harm foreseen. First aid injury but no or minimal medical treatment required	3
No impact	No injury or health & safety impact	0

Consequences - Environmental

Assessment level	Full Description	Value
Level 5 Extreme	Serious damage to the environment of national importance, and/or with prosecution certain, and/or effects not able to be fully mitigated.	85
Level 4 Major	Serious damage to the environment of national importance, and/or with prosecution expected, and/or effects able to be fully mitigated within 5 years.	35
Level 3 Significant	Serious damage to the environment of local importance, and/or with prosecution probable, and/or effects able to be fully mitigated within 1 year.	12
Level 2 Moderate	Material damage to the environment of local importance, and/or with prosecution possible, and/or effects able to be fully mitigated within 3 months.	7
Level 1 Minor	Negligible impact to the environment, and/or effects able to be fully mitigated within 1 week.	3

No Impact	No impact on the environment.	0

Consequences - Financial

Assessment level	Full Description (life of a project, not per annum)	Value
Level 5 Extreme	Cost of unplanned expenditure or loss of income or cash over $15 million	85
Level 4 Major	Cost of unplanned expenditure or loss of income or cash over $10 million	35
Level 3 Significant	Cost of unplanned expenditure or loss of income or cash over $5million	12
Level 2 Moderate	Cost of unplanned expenditure or loss of income or cash over $1 million	5
Level 1 Minor	Cost of unplanned expenditure or loss of income or cash over $500,000	2
No Financial Impact	No measurable financial impact or below $500,000	0

Likelihood

Assessment level	Full Description	Value
Almost/Near Certain	Likelihood of a Consequence occurring from an event within a 10-year period may be credibly regarded as a ‘real possibility’ i.e. the probability of occurrence is greater than non-occurrence. Expected to occur at least once within a 10-year period, i.e. a 1 in 10 year event.	95
Likely	Likelihood of a Consequence occurring from an event within a 10 year period may be credibly regarded as a ‘real possibility’ i.e. the probability of occurrence is similar to non-occurrence. There is a 50% probability of occurrence within a 10-year period, i.e. between a 1 in 10 and 1 in 20 year event.	35
Unlikely	Likelihood of a Consequence occurring from an event within a 10-year period would be considered as having some potential to occur. i.e. a reasonable probability of occurrence over time, but less than the probability of non- occurrence. Chance of occurrence is less than 50% within a 10-year period, i.e. between a 1 in 20 and a 1 in 50 year event.	12
Highly Unlikely	Likelihood of a Consequence occurring from an event whilst possible within a 10-year period would be regarded by most people as unlikely i.e. the probability of non-occurrence is somewhat larger than occurrence. Has less than 10% chance of occurrence within a 10-year period i.e. between a 1 in 50 and 1 in 100 year event.	5
Rare	The Likelihood of a Consequence occurring from an event is not expected within a 10-year period. Occurrence of the event would probably be regarded as unusual. (The probability of occurrence is quite small). Has less than 1% chance of occurrence in a 10-year period., i.e. a 1 in 100 year event	2

Appendix 2 - Sources and types of risks

When identifying risks, all sources of potential risk should be considered. The sources and types of risks are summarised, there may be other sources of risk that might be included as the council's risk management framework continues to evolve.

The following are the contextual risk categories as set out in figure 3, expanded here with some examples:

Description of risk source	Context details	Examples of some types of risk
Loss, failure or damage to assets	GWRC is responsible for managing almost $1 billion of assets. These are spread across its activities and include assets such as flood protection works, rail and water supply infrastructure, parks and forests. These are exposed to a series of risks, the source of which is sometimes outside of our control e.g. natural hazards. Maintaining these assets in a cost effective manner to provide the best possible service to our community is controlled mainly by our asset management plans together with regular monitoring and maintenance.	Water capacity insufficient to meet security of supply standard Failure of flood protection structures and measures due to flooding/earthquake
Services are severely curtailed	GWRC provides critical services, the curtailment to which can cause significant disruption and/or hardship to the community. The most significant curtailments would be a major loss of water supply or public transport. Other services include harbour navigation, resource consent management, flood monitoring alerts, all of which can be affected by outages that would cause varying degrees of distress.	Failure of GWRC's telephony system Damage to Water supply infrastructure from an event which interrupts supply Loss of the provision of IT services Bus, ferry or rail services suffer major disruption caused by severe weather or adverse environmental conditions
Physical harm to the general public	GWRC is responsible for a variety of activities and infrastructure that have the potential to harm members of the general public. Risks range from those that we have a direct relationship to the general public (e.g. maintaining our assets) to those where the direct relationship is managed by contractors for whom we are responsible (e.g. Transdev's management of rail services, KiwiRail management of the tracks).	Harm to staff , contractors when carrying out aerial pest control operations Infrastructure in parks fails Failure of KiwiRail network assets or network operations causes serious injury

Health and safety of staff and contractors & volunteers	GWRC staff, contractors & volunteers are exposed to a series of hazards potentially affecting their personal safety. Most of the significant hazards are in external environments and the work activities performed. Many of these hazards cannot be eliminated and risk is mitigated as much as is reasonably practicable.	Failure to provide a safe work environment Rangers threatened or injured by the public whilst carrying out operations Death or severe harm to staff, contractors and/or public resulting from incidents, including asset failure Failure of GWRL rail asset causes serious injury
Financial, macroeconomic risk	Unforeseen financial impact including; loss of monies from defalcation, changes to exchange rates, interest rates, commodity prices, loss of other incomes, fines/penalties, poor investment or expenses incurred.	Failure of flood protection structures and measures due to flooding Loss of Council funds due to fraud
Subsidiary companies and trusts	GWRC has several subsidiaries, namely CentrePort Ltd, WRC Holdings Ltd, Port Investments Ltd, Greater Wellington Rail Ltd and Wellington Water, Wellington Regional Economic Development Agency, Local Government Funding Agency, Ltd. GWRC was the settlor and is a trustee of the Wellington Regional Stadium Trust. Ownership of these companies exposes GWRC to risk.	CentrePort gets into financial difficulty Damage to infrastructure beyond insured levels requiring Council support
Legislative and regulatory	Failure to follow regulatory obligations, non-compliance in terms of the Acts GWRC operates under.	Failure to provide a safe work environment Water supply fails to meet NZ drinking water standards resulting in public health issues A major disaster impacts on the capacity and capability of emergency management to meet its statutory obligations The Electoral Officer is required to re-run an election process
Political	Any action or event that could bring GWRC into disrepute. Including but not limited to service delivery failure, damage or harm to the public, decision making process leading to public challenge.	All risks have a degree of political impact depending on their effect with the community

Projects	GWRC is exposed to the risk associated with the implementation and management of projects. Risks arise due to a number of factors and the project management policy requires that risks are identified as part of the project documentation process.	Major transport projects Flood protection projects Failure to deliver on key projects
Environmental damage	Significant damage to the environment either through GWRC actions or lack of actions.	Hazardous and toxic materials not identified Water quality containments Environmental damage caused by operations
Human resources	Poor staff engagement and retention, poor recruitment practices or a failure to anticipate future resourcing, competency and leadership requirements will adversely impact on GWRC's ability to operate effectively and efficiently.	Inability to attract and retain skilled staff Ineffective employment relations Inadequate human resource planning Poor staff knowledge, skills, engagement