

Table of Contents

- Introduction.....2
- Governance3
 - Framework Review3
 - Operating Model.....3
 - First line of defence*3
 - Second line of defence*.....3
 - Third line of defence*.....4
 - Governance Structure.....5
 - Roles and Responsibilities.....6
 - Document Structure (Framework).....7
- Risk Management Procedures8
 - A: Scope, Context, Criteria.....9
 - Organisational Criteria9
 - Scope and Context9
 - B: Risk Identification.....10
 - C: Risk Analysis11
 - Step 1: Determine the Inherent Risk Rating11
 - Step 2: Identify and consider the effectiveness of key controls11
 - Step 3: Determine the Residual Risk Rating.....12
 - D: Risk Evaluation12
 - E: Risk Treatment12
 - F: Communication & Consultation13
 - G: Monitor & Review13
 - H: Recording & Reporting13
 - Strategic Risks14
 - Operational Risks14
 - Identification.....15
 - Validity of Source15
 - Monitor & Review.....15
- Risk Acceptance.....16
- Appendix A- Risk Assessment and Acceptance Criteria17

Introduction

The Town of Claremont's (**Town**) Risk Management Policy in conjunction with the components of this document encompasses the Town's Risk Management Framework. It sets out the Town's approach to the identification, assessment, management, reporting and monitoring of risks. All components of this document are based on AS/NZS ISO 31000:2018 Risk management - Guidelines.

It is essential that all areas of the Town adopt these procedures to ensure:

- Strong corporate governance.
- Compliance with relevant legislation, regulations and internal policies.
- Integrated Planning and Reporting requirements are met.
- Uncertainty and its effects on objectives is understood.

This Framework aims to balance a documented, structured and systematic process with the current size and complexity of the Town.

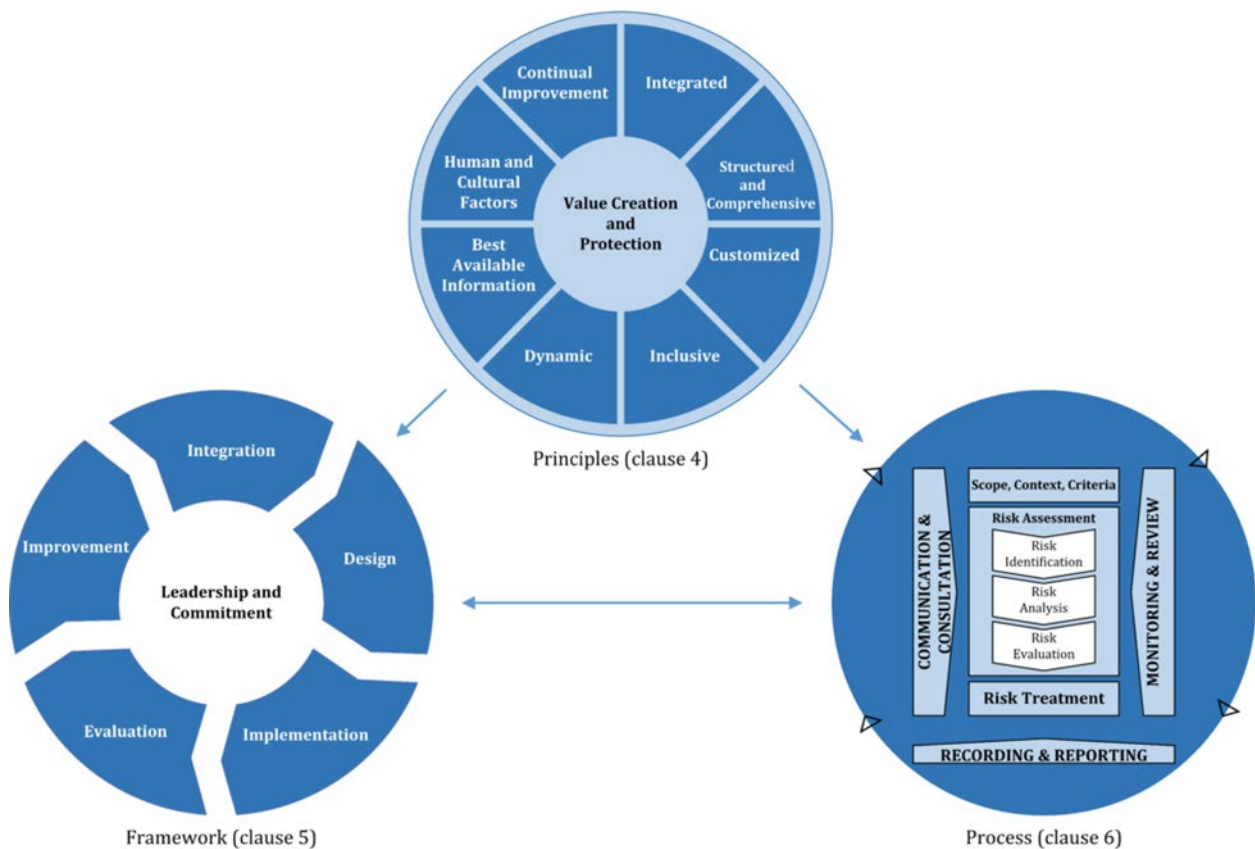


Figure 1: Relationship between the risk management principles, framework and process (Source: ISO 31000:2018)

Governance

Appropriate governance of risk management within the Town provides:

- Transparency of decision making.
- Clear identification of the roles and responsibilities of the risk management functions.
- An effective Governance Structure to support the risk framework.

Framework Review

The Risk Management Framework is to be reviewed for appropriateness and effectiveness at least every three years.

Operating Model

The Town has adopted a “Three Lines of Defence” model for the management of risk. This model ensures roles, responsibilities and accountabilities for decision making are structured to demonstrate effective governance and assurance. By operating within the approved risk appetite and framework, the Council, Management and Community will have assurance that risks are managed effectively to support delivery of the Town’s Strategic, Corporate & Operational Plans.

First line of defence

All operational areas of the Town are considered ‘1st Line’. They are responsible for ensuring that risks within their scope of operations are identified, assessed, managed, monitored and reported. Ultimately, they bear ownership and responsibility for losses or opportunities from the realisation of risk. Associated responsibilities include;

- Establishing and implementing appropriate processes and controls for the management of risk (in line with these procedures).
- Undertaking adequate analysis (data capture) to support the risk decision-making process.
- Prepare risk acceptance proposals where necessary, based on the level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second line of defence

The Executive Team act as the primary ‘2nd Line’. The Directors own and manage the framework for risk management. They draft, implement and approve the governance procedures and provide the necessary tools and training to support the 1st line process.

Maintaining oversight on the application of the framework provides a transparent view and level of assurance to the 1st & 3rd lines on the risk and control environment. Support can be provided by additional oversight functions completed by other 1st Line Teams (where applicable). Additional responsibilities include:

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinating the Town’s risk reporting for the CEO & Senior Management Team and the Audit and Risk Management Committee (**Audit Committee**).

Third line of defence

Internal & External Audits are the third line of defence, providing independent assurance to the Council, Audit Committee and Town Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

- Internal Audit – Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the CEO with input from the Audit Committee.
- External Audit – Appointed by Council on the recommendation of the Audit Committee to report independently to the Mayor and CEO on the annual financial statements only.

Governance Structure

The following diagram depicts the current operating structure for risk management within the Town.

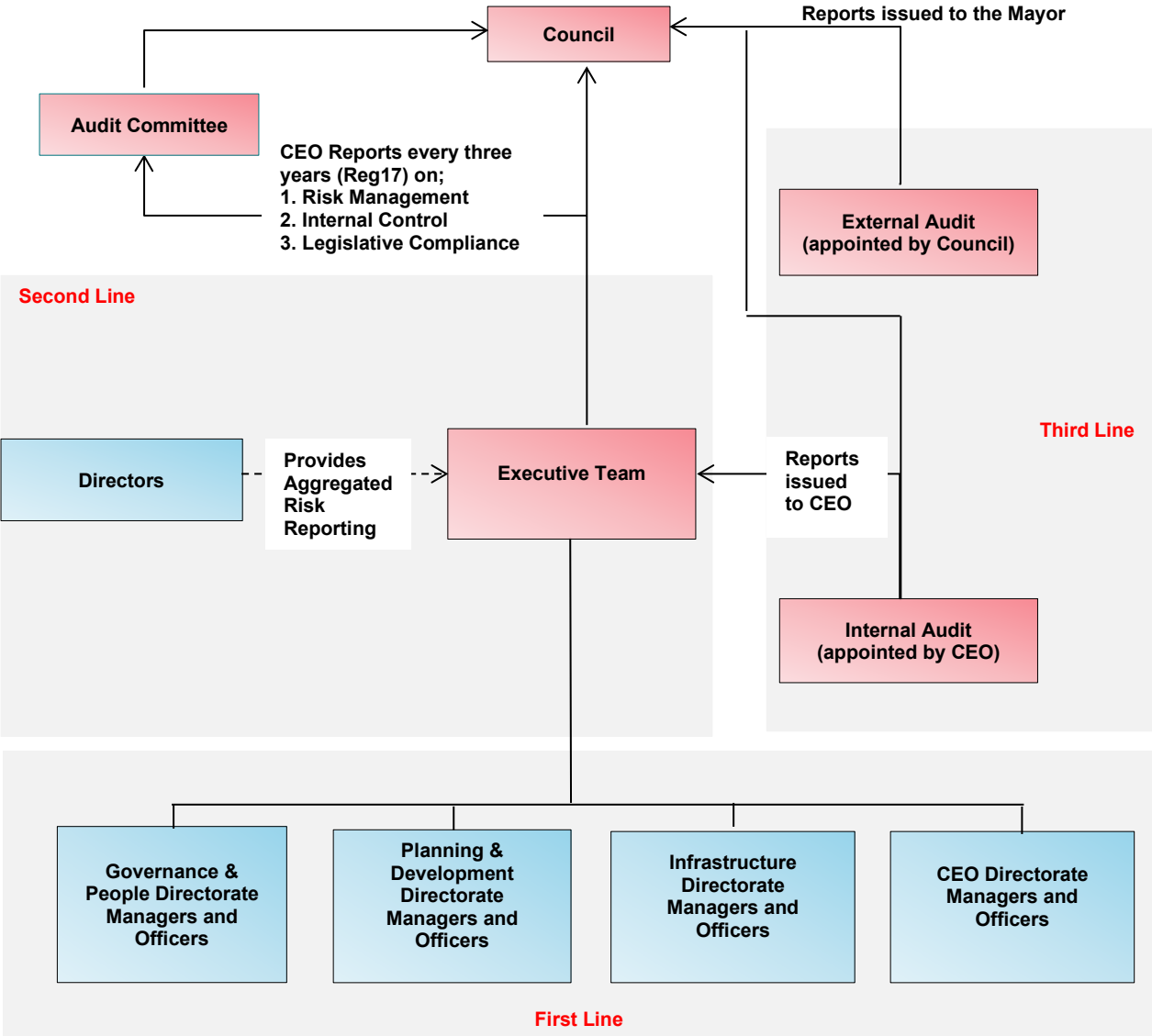


Figure 2: Operating Model

Roles and Responsibilities

Chief Executive Officer

The Chief Executive Officer (**CEO**) is the overall sponsor of the risk management process and will set the tone and promote a positive risk management culture by providing firm and visible support for risk management.

The CEO will review the appropriateness and effectiveness of the Town's systems and procedures in regard to risk management, internal controls and legislative compliance at least once every three calendar years and report the results of that review to the Audit Committee.

Executive Team

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

The Executive Team will drive the risk management process for the organisation by liaising with key stakeholders in both identifying risks, and in the recommendation of further actions to be implemented.

The Executive Team is responsible for overall reporting on the Town's Risk Management Framework, and in the evaluation of the Town's internal controls.

Management Team

Members of the Management Team are responsible for completing risk management actions for risks identified within their areas. This will be done through liaising and communication of requirements to their relevant staff members and overseeing the action to completion.

Employees

All employees within the Town are expected to develop an understanding and awareness of risks and how they can contribute to the risk management process. All employees are responsible for escalating/communicating risks to their immediate supervisor. Employees are also required to act in a manner that does not place at risk the health and safety of themselves, other employees, residents and or visitors to the Town.

Document Structure (Framework)

The following diagram depicts the relationship between the Risk Management Policy, Procedures and supporting documentation and reports.

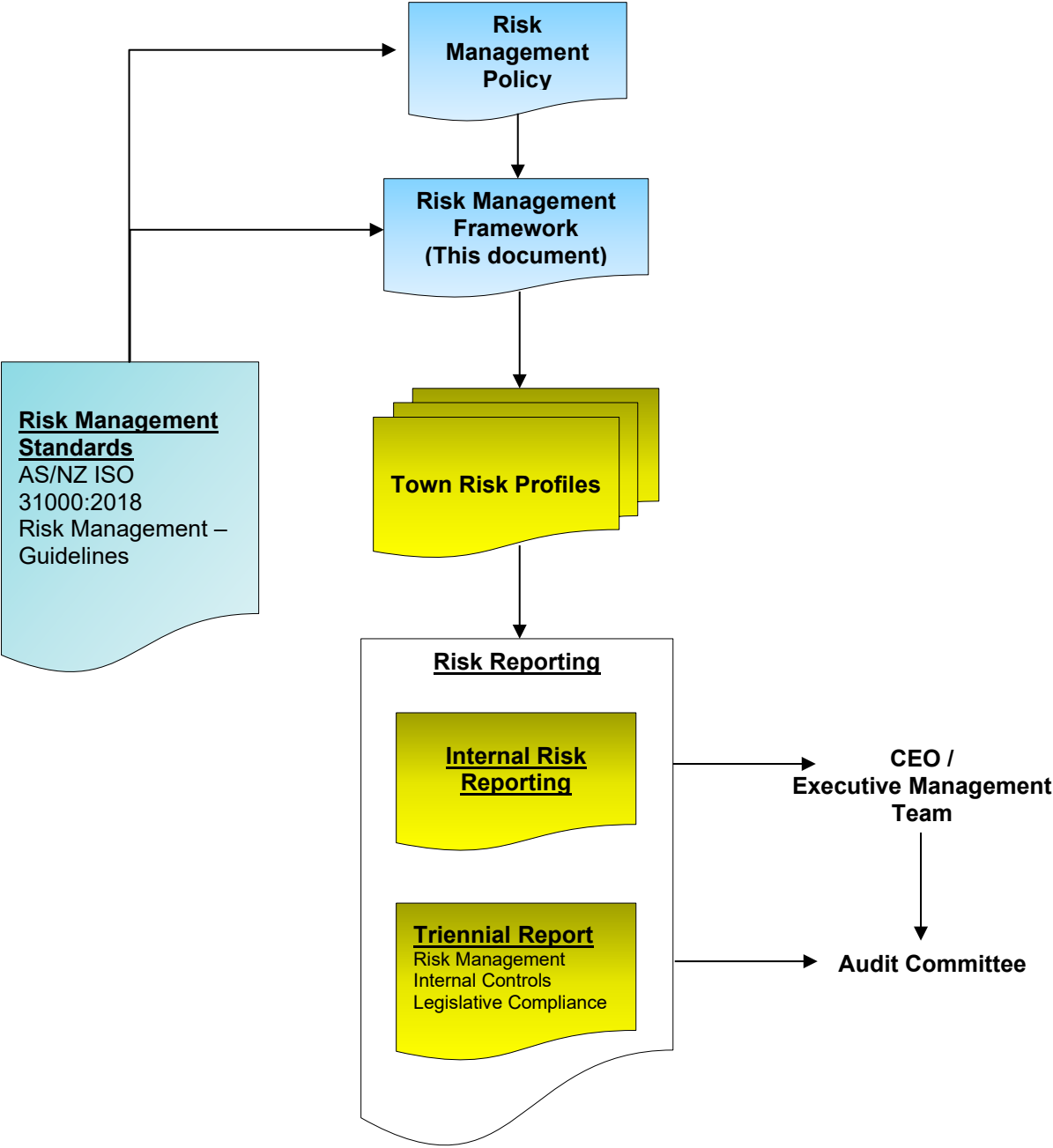


Figure 3: Document Structure

Risk Management Procedures

Each Director (assigned as the Control Owner), is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Town.
- Reviewed on at least an 18 month rotation, or sooner if there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

This process is supported by the use of key data inputs, workshops and ongoing business engagement.

The risk management process is standardised across all areas of the Town. The following diagram outlines that process with the following commentary providing broad descriptions of each step.

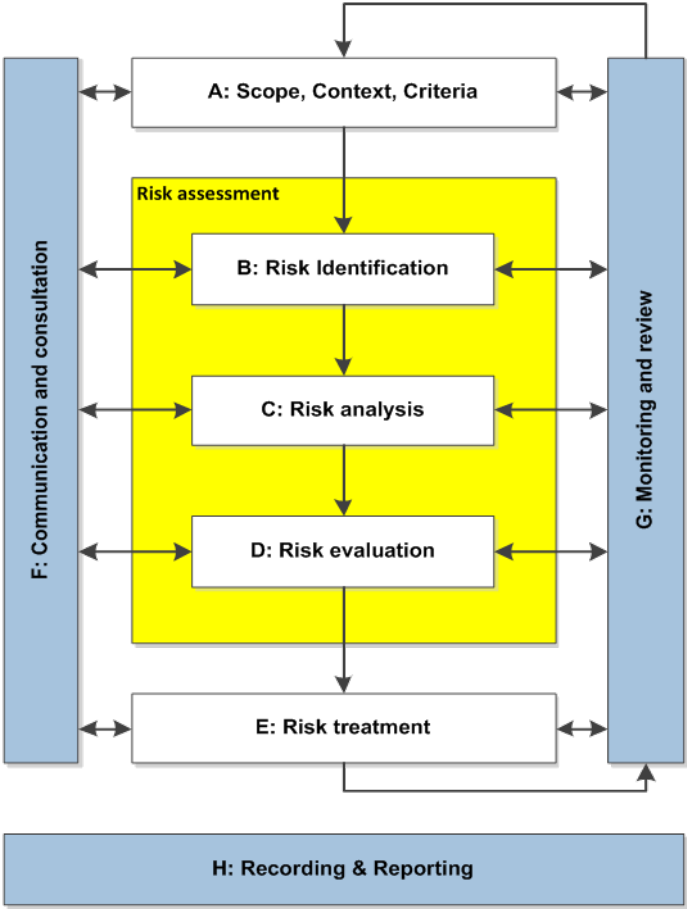


Figure 4: Risk Management Process ISO 31000:2018

A: Scope, Context, Criteria

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed, this forms two elements:

Organisational Criteria

This includes the Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed.

All risk assessments are to utilise these documents to allow consistent and comparable risk information to be developed and considered within planning and decision-making processes.

Scope and Context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. Risk sources can be internal or external.

For specific risk assessment purposes the Town has three levels of risk assessment context:

(i) Strategic Context

These risks are associated with achieving the organisation's long term objectives. Inputs to establishing the strategic risk assessment context may include;

- Organisational Values / Vision.
- Stakeholder Analysis.
- Environment Scan / SWOT Analysis.
- Strategies / Objectives / Goals (Integrated Planning & Reporting).

The Town's Integrated Strategic planning documents captures the identification and management of its strategic risks.

(ii) Operational Context

The Town's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its key activities i.e. what is it aiming to achieve? In addition, existing Risk Profiles are to be utilised where possible to assist in the identification of related risks.

These Risk Profiles are expected to change over time. In order to ensure consistency, any amendments must be approved by the Executive Team.

(iii) Project Context

Project Risk has two main components:

- Direct refers to the risks that may arise as a result of project activity (i.e. impacting on process, resources or IT systems), which may prevent the Town from meeting its objectives.
- Indirect refers to the risks which threaten the delivery of project outcomes.

In addition to understanding what is to be assessed, it is also important to understand who are the key stakeholders or areas of expertise that may need to be included within the risk assessment.

B: Risk Identification

Once the context has been determined, the next step is to identify risks. This is the process of finding, recognising and describing risks. Risks are described as the point along an event sequence where control has been lost. An event sequence is shown below:

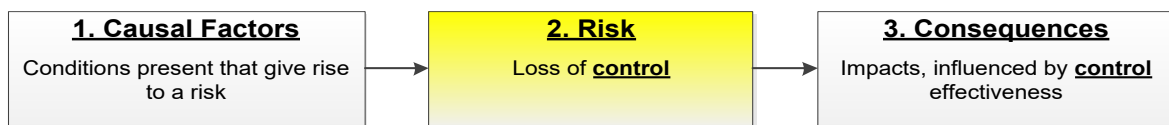


Figure 5: Event (risk) sequence

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, raise the questions listed below and then capture and review the information within each defined Risk Profile. The objective is to identify potential risks that could stop the Town from achieving its goals. This step is also where opportunities for enhancement or gain across the organisation can be found.

These questions / considerations should be used only as a guide, as unidentified risks can cause major losses through missed opportunities or adverse events occurring. Additional analysis may be required.

Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

'Brainstorming' will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are considered to be the subject experts when considering potential risks to the objectives of the work environment and should be included in all risk assessments being undertaken.

Key risks can then be identified and captured within the Risk Profiles.

- What can go wrong? / What are areas of uncertainty? (**Risk Description**)
- How may this risk eventuate? (**Potential Causes**)
- What are the current measurable activities that mitigate this risk from eventuating? (**Controls**)
- What are the potential consequential outcomes of the risk eventuating? (**Consequences**)

Risk Description – describe what the risk is and specifically where control may be lost. They can also be described as an event. They are not to be confused with outcomes following an event, or the consequences of an event.

Potential Causes – are the conditions that may present or the failures that may lead to the event, or point in time when control is lost (risk).

Controls – are measures that modify risk. At this point in the process only existing controls should be considered. They must meet the following three tests to be considered as controls:

1. Is it an object, technological system and / or human action?
2. Does it, by itself, arrest or mitigate an unwanted sequence?
3. Is the required performance specifiable, measureable and auditable?

Consequences – need to be impacts to the Town. These can be staff, visitor or contractor injuries; financial; interruption to services; non-compliance; damage to reputation or assets or the environment. There is no need to determine the level of impact at this stage.

C: Risk Analysis

To analyse identified risks, the Town's Risk Assessment and Acceptance Criteria (Appendix A) is now applied.

Step 1: Determine the Inherent Risk Rating

There are three components to this step:

1. Determine relevant consequence categories and rate the 'probable worst consequence' if the risk eventuated without controls in place. This is not the worst case scenario but rather a qualitative judgement of the worst scenario that is probable or foreseeable. (Consequence)
2. Determine how likely it is that the 'probable worst consequence' will eventuate without controls in place. (Likelihood)
3. Using the Town's Risk Matrix, combine the measures of consequence and likelihood to determine the risk rating. (Risk Rating)

Step 2: Identify and consider the effectiveness of key controls

Controls need to be considered from three perspectives:

1. The design effectiveness of each individual key control.
2. The operating effectiveness of each individual key control.
3. The overall or combined effectiveness of all identified key controls.

Design Effectiveness

This process reviews the 'design' of the controls to understand their potential for mitigating the risk without any 'operating' influences. Controls that have inadequate designs will never be effective, no matter if it is performed perfectly every time.

There are four components to be considered in reviewing existing controls or developing new ones:

1. *Completeness* – The ability to ensure the process is completed once. How does the control ensure that the process is not lost or forgotten, or potentially completed multiple times?
2. *Accuracy* – The ability to ensure the process is completed accurately, that no errors are made or components of the process missed.
3. *Timeliness* – The ability to ensure that the process is completed within statutory timeframes or internal service level requirements.
4. *Theft or Fraud* – The ability to protect against internal misconduct or external theft / fraudulent activities.

It is very difficult to have a single control that meets all the above requirements when viewed against a Risk Profile. It is imperative that all controls are considered so that the above components can be met across a number of controls.

Operating Effectiveness

This process reviews how well the control design is being applied. Similar to above, the best designed control will have no impact if it is not applied correctly. As this generally relates to the human element of control application there are four main approaches that can be employed by management or the risk function to assist in determining the operating effectiveness and / or performance management.

- *Re-perform* – this is only applicable for those short timeframe processes where they can be re-performed. The objective is to re-perform the same task, following the design to ensure that the same outcome is achieved.

- *Inspect* – review the outcome of the task or process to provide assurance that the desired outcome was achieved.
- *Observe* – physically watch the task or process being performed.
- *Inquire* – through discussions with individuals / groups determine the relevant understanding of the process and how all components are required to mitigate any associated risk.

Overall Effectiveness

This is the value of the combined controls in mitigating the risk. All factors as detailed above are to be taken into account so that a considered qualitative value can be applied to the 'control' component of risk analysis.

The criterion for applying a value to the overall control is the same as for individual controls and can be found in Appendix A under 'Existing Control Ratings'.

Step 3: Determine the Residual Risk Rating

There are three components to this step:

1. Determine relevant consequence categories and rate the 'probable worst consequence' if the risk eventuated with existing controls in place. This is not the worst case scenario but rather a qualitative judgement of the worst scenario that is probable or foreseeable. (Consequence)
2. Determine how likely it is that the 'probable worst consequence' will eventuate with existing controls in place. (Likelihood)
3. Using the Town's Risk Matrix, combine the measures of consequence and likelihood to determine the risk rating. (Risk Rating)

D: Risk Evaluation

Risk evaluation takes the residual risk rating and applies it to the Town's Risk Acceptance Criteria (Appendix A) to determine whether the risk is within acceptable levels to the Town.

The outcome of this evaluation will determine whether the risk is low; moderate; high or extreme.

It will also determine through the use of the Risk Acceptance Criteria, what (if any) high level actions or treatments need to be implemented.

Note: Individual Risks or Issues may need to be escalated due to urgency, level of risk or of a systemic nature.

E: Risk Treatment

There are generally two requirements following the evaluation of risks.

1. In all cases, regardless of the residual risk rating; controls that are rated 'Inadequate' must have a treatment plan (action) to improve the control effectiveness to at least 'Adequate'.
2. If the residual risk rating is high or extreme, treatment plans must be implemented to either:
 - a. Reduce the consequence of the risk materialising.
 - b. Reduce the likelihood of occurrence.

(Note: these should have the desired effect of reducing the risk rating to at least moderate)

 - c. Improve the effectiveness of the overall controls to 'Effective' and obtain delegated approval to accept the risk as per the Risk Acceptance Criteria.

Once a treatment has been fully implemented, the CEO is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (Refer to Risk Acceptance section).

F: Communication & Consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk, and those with a vested interest, understand the basis on which decisions are made and why particular treatment / action options are selected or the reasons to accept risks have changed.

As risk is defined as the effect of uncertainty on objectives, consulting with relevant stakeholders assists in the reduction of components of uncertainty. Communicating these risks and the information surrounding the event sequence ensures decisions are based on the best available knowledge.

G: Monitor & Review

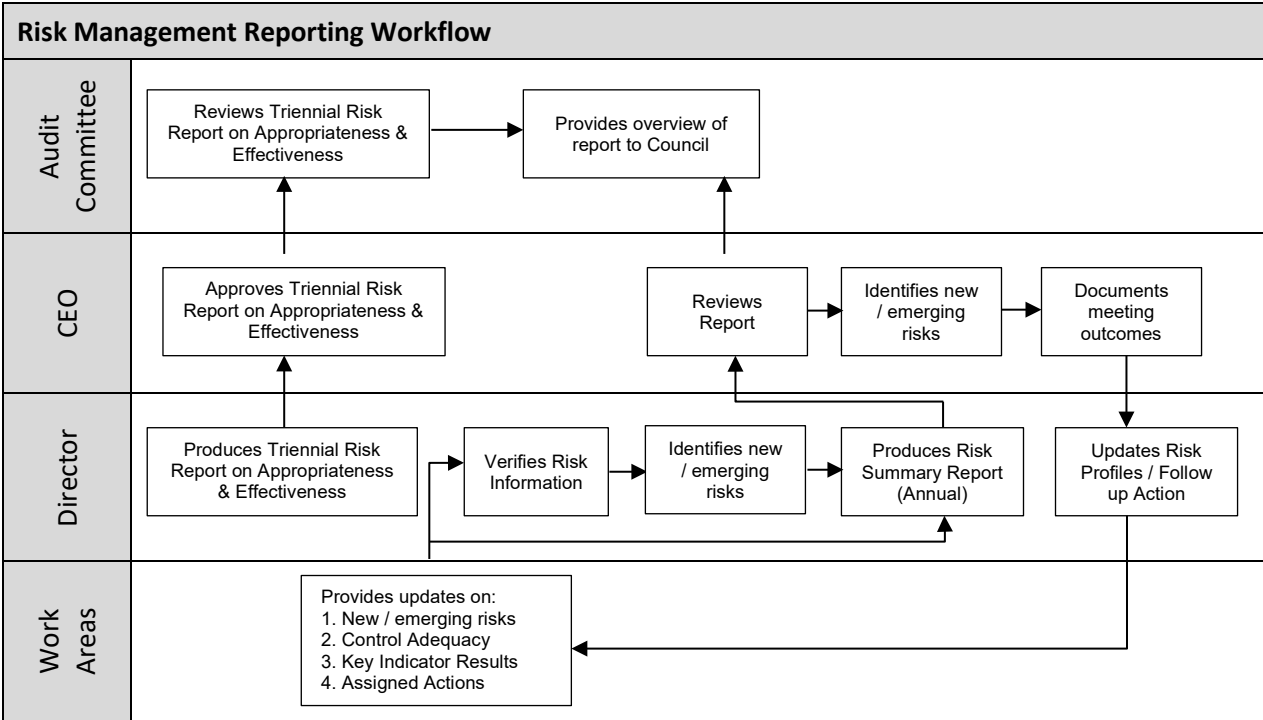
It is essential to monitor and review the management of risks, as changing circumstances may result in some risks increasing or decreasing in significance.

By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, we can determine if the organisation’s resources are being put to the best use possible.

During the quarterly reporting process, management are required to review any risks within their area and follow up on controls and treatments / action mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also apply to any actions / treatments to originate from an internal audit. The audit report will provide recommendations that effectively are treatments for risks that have been tested during an internal review.

H: Recording & Reporting

The following diagram provides a high level view of the ongoing reporting process for Risk Management.



Each Work Area is responsible for ensuring:

- They continually provide updates in relation to new, emerging risks, control effectiveness and any relevant key indicator performance to the Director.
- Work through assigned actions and provide relevant updates to the Director
- Risks / Issues reported to the CEO & Executive Team are reflective of the current risk and control environment.

The Director/s are responsible for:

- Ensuring Town Risk Profiles are formally reviewed and updated, at least on an 18 month rotation or earlier when there has been a material restructure, change in risk ownership or change in the external environment.
- Annual Risk Reporting for the CEO & Executive Team – Contains an overview of the Risk Summary for the Town.

Audit Committee

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

Risk Profiles

Strategic Risks

The Town captures its strategic risks through the development and implementation of the Town's Strategic Plan.

Operational Risks

- | | | |
|---|--|------------------------------------|
| • Asset Sustainability | • Business and Community Disruption | • Compliance Obligations |
| • Document Management | • Employment Practices | • Community Engagement |
| • Environment Management | • Errors, Omissions and Delays | • External Theft and Fraud |
| • Management of Facilities, Venues and Events | • IT, Communication Systems and Infrastructure | • Misconduct |
| • Project / Change Management | • Safety & Security Practices | • Supplier and Contract Management |

The Town utilises risk profiles to capture its operational risks. The profiles assessed are:

For each category, the profile contains the following:

- Objective.
- Risk Event.
- Potential Causes.

- Key Controls / Control Type .
- Control Adequacy.
- Control owner.
- Risk Rating.
- Actions and Responsibility.

Key Indicators

Key Indicators may be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of Key Indicators:

- Identification.
- Validity of Source.
- Tolerances.
- Monitor & Review.

Identification

The following represent the minimum standards when identifying appropriate Key Indicators:

- The risk description and casual factors are fully understood
- The Key Indicator is fully relevant to the risk or control
- Predictive Key Indicators are adopted wherever possible
- Key Indicators provide adequate coverage over monitoring key risks and controls

Validity of Source

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the Key Indicator data is relevant to the risk or control.

Where possible the source of the data (data owner) should be independent to the risk owner. Overlapping Key Indicators can be used to provide a level of assurance on data integrity.

If the data or source changes during the life of the Key Indicator, the data is required to be revalidated to ensure reporting of the Key Indicator against a consistent baseline.

Monitor & Review

All active Key Indicators are updated as per their stated frequency of the data source.

When monitoring and reviewing Key Indicators, the overall trend must be considered over a longer timeframe than that of individual data movements only. The trend of the Key Indicators is specifically used as an input to the risk and control assessment.

Risk Acceptance

Day to day operational management decisions are generally managed under the delegated authority framework of the Town.

Risk Acceptance is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria).

The following process is designed to provide a framework for those identified risks.

The 'Risk Acceptance' must be in writing, signed by the relevant Manager, and include:

- A description of the risk and the reasons for holding a risk outside appetite
- An assessment of the risk (e.g. Impact consequence, materiality, likelihood, working assumptions etc.)
- Details of any mitigating action plans or treatment options in place
- An estimate of the expected remediation date.

A lack of budget / funding to remediate a material risk outside appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (i.e. Executive Team)

Appendix A- Risk Assessment and Acceptance Criteria

Measures of Consequence									
Rating(Level)	Health	Financial Impact	Service Interruption	Compliance	Reputational	Property	Environment	Project TIME	Project COST
Insignificant (1)	Near miss. Minor first aid injuries	Less than \$20,000	No material service interruption	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential damage.	Contained, reversible impact managed by on site response	Exceeds deadline by 10% of project timeline	Exceeds project budget by 10%
Minor (2)	Medical type injuries	\$20,001 - \$100,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non-compliances	Substantiated, low impact, low news item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response	Exceeds deadline by 15% of project timeline	Exceeds project budget by 15%
Moderate (3)	Lost time injury < 30 days	\$100,001 - \$500,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term non-compliance but with significant regulatory requirements imposed	Substantiated, public embarrassment, moderate impact, moderate news profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies	Exceeds deadline by 20% of project timeline	Exceeds project budget by 20%
Major (4)	Lost time injury > 30 days	\$500,001 - \$1,000,000	Prolonged interruption of services – additional resources; performance affected < 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, high impact, high news profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies	Exceeds deadline by 25% of project timeline	Exceeds project budget by 25%
Catastrophic (5)	Fatality, permanent disability	More than \$1,000,000	Indeterminate prolonged interruption of services – non-performance > 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Extensive damage requiring prolonged period of restitution	Uncontained, irreversible impact	Exceeds deadline by 30% of project timeline	Exceeds project budget by 30%

Measures of Likelihood			
Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances (>90% chance)	More than once per year
4	Likely	The event will probably occur in most circumstances(>50% chance)	At least once per year
3	Possible	The event should occur at some time(20% chance)	At least once in 3 years
2	Unlikely	The event could occur at some time(<10% chance)	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances(<5% chance)	Less than once in 15 years

Risk Matrix						
Consequence		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood		1	2	3	4	5
Almost Certain	5	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely	2	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

Risk Acceptance Criteria			
Risk Rank	Description	Criteria	Responsibility
LOW	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Supervisor / Coordinator/ Team Leader
MODERATE	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Manager
HIGH	Urgent Attention Required	Risk acceptable with effective controls, managed by senior management / executive and subject to monthly monitoring	Executive Team
EXTREME	Unacceptable	Risk only acceptable with effective controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	CEO & Council

Existing Controls Ratings		
Rating	Foreseeable	Description
Effective	There is <u>little</u> scope for improvement.	Processes (Controls) operating as intended and aligned to Policies / Procedures. Subject to ongoing monitoring. Reviewed and tested regularly.
Adequate	There is <u>some</u> scope for improvement.	Processes (Controls) generally operating as intended, however inadequacies exist. Limited monitoring. Reviewed and tested, but not regularly.
Inadequate	There is a <u>need</u> for improvement or action.	Processes (Controls) not operating as intended. Processes (Controls) do not exist, or are not being complied with. Have not been reviewed or tested for some time.

Document Control Box			
Owner:	Chief Executive Officer	Business Unit:	Risk
Legislation and Other References:	<i>Local Government (Audit) Regulations 1996</i> LG534 Risk Management AS/NZ ISO 31000:2018 Risk management - Guidelines		
Document Management:			
Review Frequency:	Every three years	Next Review Date	2024
Version Control	Approval Date	Reference	
1.	8 February 2022	Council Resolution 006/22	