Audit and Governance Committee - Wednesday, 4 September 2024 Attachments

MINUTES

Audit and Governance Committee

Wednesday 12 June 2024, 5:30 pm

in the Council Chamber,
Administration Building
48 Old Perth Road, Bassendean

1 Declaration Of Opening; Acknowledgment of Country; Acknowledgment of Visitors; Disclaimer

The Presiding Member declared the meeting open at 5:06pm, welcomed all those in attendance and acknowledged the past and present traditional owners and custodians of the land on which the meeting was held.

2 Announcements by the Presiding Member without Discussion

Nil

3 Attendances, Apologies and Leave of Absence

Present

Councillors

Cr Kathryn Hamilton, Mayor (Presiding Member)
Cr Paul Poliwka, Deputy Mayor (via Electronic Means)

Officers

Mr Paul White, Director Corporate Services
Ms Joanne Burges, Manager Governance & Strategy
Ms Waruni De Silva, Manager Financial Services
Mr Tristan Loney, Manager Information and Technology

Community Member

Ms Sasha Rademakers

Paxon

Ian Ekins, Associate Director (via Electronic Means)

Public

There were no members of the public in attendance.

Apologies

Cr Ken John
Cr Jamayne Burke
Mr Ron Back

4 Declarations of Interest

Nil

5 Presentations or Deputations

6 Confirmation of Minutes

Council Resolution/Officer Recommendation – Item 6.1

MOVED Cr Kathryn Hamilton, Seconded Ms Sasha Rademakers

That the minutes of the Audit and Governance Committee meeting held on 6 March 2024, be received and confirmed as a true and correct record.

CARRIED UNANIMOUSLY 3/0

7 Business Deferred from Previous Meeting

8 Reports

8.1 Annual Audit of the Financial Report for 2023/24 - Audit Planning Memorandum	
Property Address	N/A
Landowner/Applicant	N/A
File Reference	FINM/AUD/8
Directorate	Corporate Services
Previous Reports	N/A
Authority/Discretion	**Information** For the Council/Committee to note.
Attachments	1. Updated Town of Bassendean Audit Planning Memorandum 30 June 2024 [**8.1.1** - 21 pages]

Purpose

The purpose of this report is to provide the Audit Planning Memorandum (APM) for the audit of the Town's Financial Report for 2023/24 to the Committee.

Committee/Officer Recommendation – Item 8.1

MOVED Ms Sasha Rademakers, Seconded Cr Kathryn Hamilton,

That the Audit and Governance Committee receives the RSM Audit Planning Memorandum for the audit of the Town's Financial Report for 2023/24, attached to this report.

Voting requirements: Simple Majority

CARRIED UNANIMOUSLY 3/0

8.2 Draft Audit and Governance Committee Charter	
Property Address	
Landowner/Applicant	
File Reference	GOVN/CCLMEET/1
Directorate	CEO and Council Support
Previous Reports	
Authority/Discretion	**Executive** The substantial direction setting and oversight role of the Council.
Attachments	1. Audit Committee Charter - Final Draft 310524 [**8.2.1** - 9 pages]

Purpose

The purpose of this report is for Audit and Governance Committee (Committee) to consider replacing the existing Audit and Governance Committee Instrument of Appointment and Delegation with a contemporary Audit and Governance Committee Charter.

Committee/Officer Recommendation – Item 8.2

MOVED Cr Kathryn Hamilton, Seconded Ms Sasha Rademakers,

That the Committee recommend that Council adopt the Audit and Governance Committee Charter as attached to this Report.

Voting requirements: Simple Majority

CARRIED UNANIMOUSLY 3/0

8.3 Record Keeping Policy Review	
Property Address	N/A
Landowner/Applicant	N/A
File Reference	INFM/POLCY/1
Directorate	Corporate Services
Previous Reports	N/A
Authority/Discretion	**Legislative** Includes adopting local laws, local planning schemes & policies.
Attachments	1. Draft Amended Record Keeping Policy - Tracked changes [**8.3.1** - 4 pages] 2. Draft Amended Record Keeping Policy - Clean [**8.3.2** - 4 pages]

Purpose

The purpose of this report is for the Audit and Governance Committee to consider a revised draft Record Keeping Policy for the Town.

Committee/Officer Recommendation – Item 8.3

MOVED Cr Kathryn Hamilton, Seconded Ms Sasha Rademakers,

That the Audit and Governance Committee:

1. Reviews the draft amended Record Keeping Policy attached to this report; and
2. Recommends that Council adopt the draft amended Record Keeping Policy.

Voting requirements: Simple Majority

CARRIED UNANIMOUSLY 3/0

8.4 Purchasing Policy Review	
Property Address	N/A
Landowner/Applicant	N/A

File Reference	FINM/PROCED/1
Directorate	Corporate Services
Previous Reports	12 June 2023
Authority/Discretion	**Legislative** Includes adopting local laws, local planning schemes & policies.
Attachments	1. Purchasing Policy - Marked up [**8.4.1** - 10 pages] 2. Draft Amended Purchasing Policy - June 2024 [**8.4.2** - 8 pages] 3. Purchasing Policy - LG Comparison [**8.4.3** - 4 pages]

Purpose

The purpose of this report is for the Audit and Governance Committee to review the Town's Purchasing Policy. A draft amended Purchasing Policy is attached to this report.

Committee/Officer Recommendation – Item 8.4

MOVED Ms Sasha Rademakers, Seconded Cr Kathryn Hamilton,

That the Audit and Governance Committee:

1. Inserts the following into the draft amended Purchasing Policy against the proposed $1,001 to $5,000 purchase value threshold: "*The Town will use its general knowledge of the market to ascertain whether the purchase represents value for money. The Town should seek more than one quotation if they are not satisfied that the first choice of supplier would represent value for money".*

2. Recommends Council adopt the draft amended Purchasing Policy attached to this report, as amended by resolution 1 above.

3. Notes the administration will prepare a report for the Committee within 12 months on compliance with the requirements of the Purchasing Policy, informed by its internal audit program.

Voting requirements: Simple Majority

CARRIED UNANIMOUSLY 3/0

8.5 Audit Findings Log	
Property Address	N/A
Landowner/Applicant	N/A
File Reference	GOVN/CCLMEET/1
Directorate	Corporate Services
Previous Reports	Quarterly
Authority/Discretion	**Executive** The substantial direction setting and oversight role of the Council.
Attachments	1. CONFIDENTIAL - June 2024 Audit Findings Log [**8.5.1** - 7 pages]

Purpose

The purpose of this report is to provide the Audit and Governance Committee with the Town's Audit Findings Log, with updated actions since the meeting of the Committee on 6 March 2024.

Committee/Officer Recommendation – Item 8.5

MOVED Ms Sasha Rademakers, Seconded Cr Paul Poliwka,

That the Audit and Governance Committee receives the Audit Findings Log and notes the action taken or proposed to address the recommendations.

Voting requirements: Simple Majority

CARRIED UNANIMOUSLY 3/0

9 Motions of Which Previous Notice Has Been Given

10 Announcements of Notices of Motion for the Next Meeting

11 Confidential Business

12 Closure

There being no further business, the Presiding Member declared the meeting closed, the time being 5:30 pm.

Council Policy

Risk Management Policy

Purpose

The Town of Bassendean's ("the Town") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Town's strategies, goals or objectives.

Policy Scope

This policy applies to all of the Town's activities and decision making and applies to all elected members, employees, contractors and volunteers. The policy provides a framework for the Town's strategic, operational and project risks.

Policy Statement

It is the Town's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2018 Risk management), in the management of all risks that may affect the Town, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Town's Integrated Planning Framework.

The Town's Corporate Management Committee will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee, elected member, volunteer and contractor within the Town is recognised as having a role in risk management.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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 the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, strategies, goals and objectives.

- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.
- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Town defined its risk appetite through the development and endorsement of the Town's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All strategic risks to be reported at a corporate level are to be assessed according to the Town's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Corporate Management Committee.

Roles, Responsibilities & Accountabilities

Council's role is to -

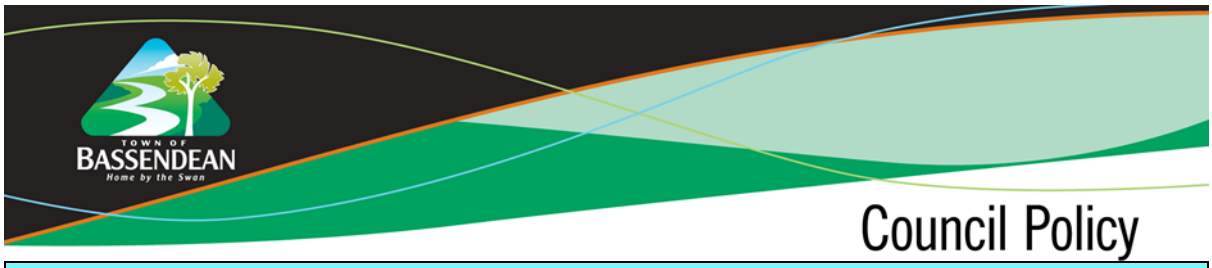
- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the Local Government Act.

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town will implement and integrate a monitor and review process to report on the achievement of the Risk Management Objectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be kept under review by the Town's Corporate Management Committee and will be formally reviewed by Council biennially.



Document Control box			
Document Responsibilities:			
Owner:	Chief Executive Officer	**Owner Business Unit:**	Office of the Chief Executive Officer
Inception Date:	OCM-14/3/2022	**Decision Maker:**	Council
Review Date:	Biennial	**Repeal and Replace:**	N/A
Compliance Requirements:			
Legislation:	***Local Government Act 1995***		

Risk Management Policy

Purpose

The Town of Bassendean's ("the Town") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Town's strategies, goals or objectives.

Policy Scope

This policy applies to all of the Town's activities and decision making and applies to all ~~elected~~ council members, employees, contractors and volunteers. The policy provides a framework for the Town's strategic, operational and project risks.

Policy Statement

It is the Town's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2018 Risk management), in the management of all risks that may affect the Town, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Town's Integrated Planning Framework.

The Town's Corporate Management Committee will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee, ~~elected~~ council member, volunteer and contractor within the Town is recognised as having a role in risk management.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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 the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.
- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Town defined its risk appetite through the development and endorsement of the Town's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All strategic risks to be reported at a corporate level are to be assessed according to the Town's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Corporate Management Committee.

Roles, Responsibilities & Accountabilities

Council's role is to -

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

Formatted: Font: Italic

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town will implement and integrate a monitor and review process to report on the achievement of the Risk Management ~~Objectives~~objectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be kept under review by the Town's Corporate Management Committee and will be formally reviewed by Council biennially.

Document responsibilities:			
Owner:	~~COUNCIL~~Chief Executive Officer	**Owner Business Unit:**	Office of the CEO
Inception date:	OCM 22/03/2022	**Decision maker:**	Council
Review Date:	OCM 24/09/2024	**Repeal and replace:**	N/A
Review Frequency	Biennial		
Compliance Requirements: ***Local Government (Audit) Regulations,*** **Regulation 17**			
Legislation	***Local Government Act 1995***		

Formatted: Not Highlight

Formatted: Font color: Red

Formatted: Not Highlight

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Risk Management Policy

Purpose

The Town of Bassendean's ("the Town") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Town's strategies, goals or objectives.

Policy Scope

This policy applies to all of the Town's activities and decision making and applies to all council members, employees, contractors and volunteers. The policy provides a framework for the Town's strategic, operational and project risks.

Policy Statement

It is the Town's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2018 Risk management), in the management of all risks that may affect the Town, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Town's Integrated Planning Framework.

The Town's Corporate Management Committee will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee, council member, volunteer and contractor within the Town is recognised as having a role in risk management.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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 the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.
- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Town defined its risk appetite through the development and endorsement of the Town's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All strategic risks to be reported at a corporate level are to be assessed according to the Town's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Corporate Management Committee.

Roles, Responsibilities & Accountabilities

Council's role is to -

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town will implement and integrate a monitor and review process to report on the achievement of the Risk Management objectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be kept under review by the Town's Corporate Management Committee and will be formally reviewed by Council biennially.

Document responsibilities:			
Owner:	Chief Executive Officer	**Owner Business Unit:**	Office of the CEO
Inception date:	OCM 22/03/2022	**Decision maker:**	Council
Review Date:	OCM 24/09/2024	**Repeal and replace:**	N/A
Review Frequency	Biennial		
Compliance Requirements: ***Local Government (Audit) Regulations,*** **Regulation 17**			
Legislation	***Local Government Act 1995***		

Town of Bassendean

Risk Management Framework

- Risk Management Policy
- Risk Management Procedures

CONFIDENTIAL

~~February 2022~~September 2024

Version: ~~1.0~~2.0

Table of Contents

VERSION CONTROL			
Number	**Date**	**Item**	**Reason**
1	15/12/2022	Measures of Consequence Table	Amended measures of consequence table financial impact at minor amended from $10,000 - $50,000, to $15,001 - $50,000'. Major amended from $200,000 to $500,000' to '$200,001 to $500,000'.
2	04/09/2024	Administrative Review	Amended 'elected members' to Council Members for contemporary reference. Minor administrative amendments to organisational structure and process charts throughout.
3			
4			
5			
6			
7			

Introduction

The Policy and Procedures form the Risk Management Framework for the Town of Bassendean ("the Town"). 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 Australia/New Zealand Standard ISO 31000:2018 Risk Management – Principles and 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 along with existing time, resource and workload pressures.

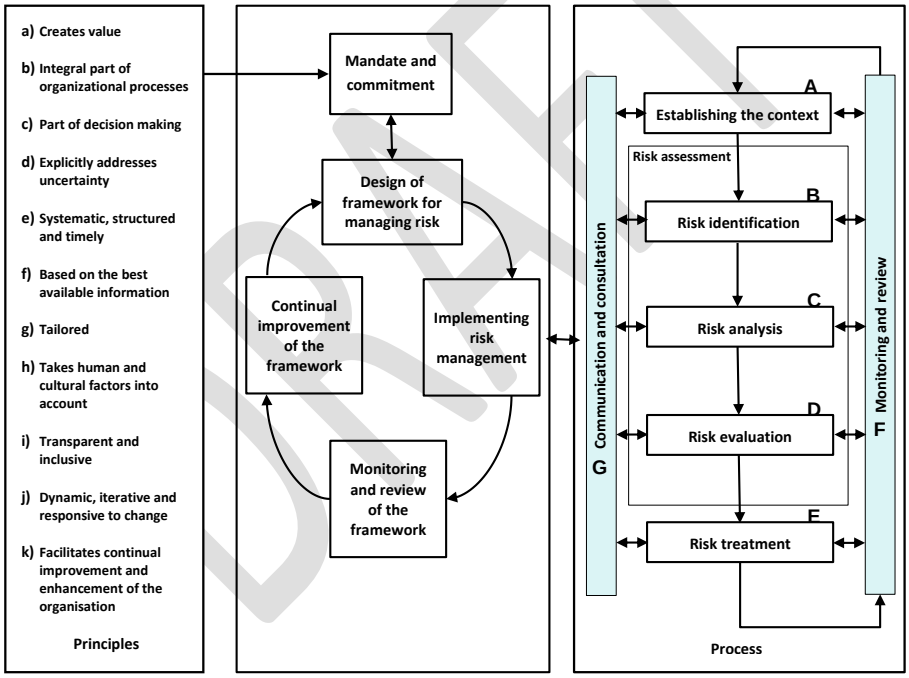


Figure 1: Risk Management Process (Source: AS/NZS 31000:2018)

Risk Management Policy

Purpose

The Town of Bassendean's ("the Town") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Town's strategies, goals or objectives.

Policy Scope

This policy applies to all of the Town's activities and decision making and applies to all ~~elected~~ Council M~~m~~embers, employees, contractors and volunteers. The policy provides a framework for the Town's strategic, operational and project risks.

Policy Statement

It is the Town's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2018 Risk management), in the management of all risks that may affect the Town, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Town's Integrated Planning Framework.

The Town's Corporate Management Committee will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee, ~~elected~~ Council M~~m~~ember, volunteer and contractor within the Town is recognised as having a role in risk management.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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 the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.

- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Town defined its risk appetite through the development and endorsement of the Town's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All strategic risks to be reported at a corporate level are to be assessed according to the Town's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Corporate Management Committee.

Roles, Responsibilities & Accountabilities

Council's role is to:

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town will implement and integrate a monitor and review process to report on the achievement of the Risk Management oObjectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be kept under review by the Town's Corporate Management Committee and will be formally reviewed by Council biennially.

Document Control box			
Document Responsibilities:			
Owner:	Chief Executive Officer	**Owner Business Unit:**	Office of the Chief Executive Officer
Inception Date:	OCM 22/03/2022	**Decision Maker:**	Council
Review Date:	Biennial	**Repeal and Replace:**	N/A
Review Frequency	September 2026		

Formatted: Font: Italic

Formatted: Font: Italic

Formatted Table

Compliance Requirements:	
Legislation:	***Local Government Act 1995***

Risk Management Procedures

Governance

Appropriate governance of risk management within the Town of Bassendean (the "Town") provides:

- Transparency of decision making.
- Clear identification of the roles and responsibilities of 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 biennially.

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 the delivery of Strategic and 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 decision-making process of risk.
- Prepare risk acceptance proposals where necessary, based on level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Town's Risk Framework Owner (Manager Governance and Strategy) acts as the primary **'2nd Line'**. This position owns and manages the framework for risk management, drafts and implements governance procedures and provides the necessary tools and training to support the 1st line process. The Corporate Management Committee supplements the second line of defence.

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 & Corporate Management Committee and the Audit and Governance Committee.

Third Line of Defence

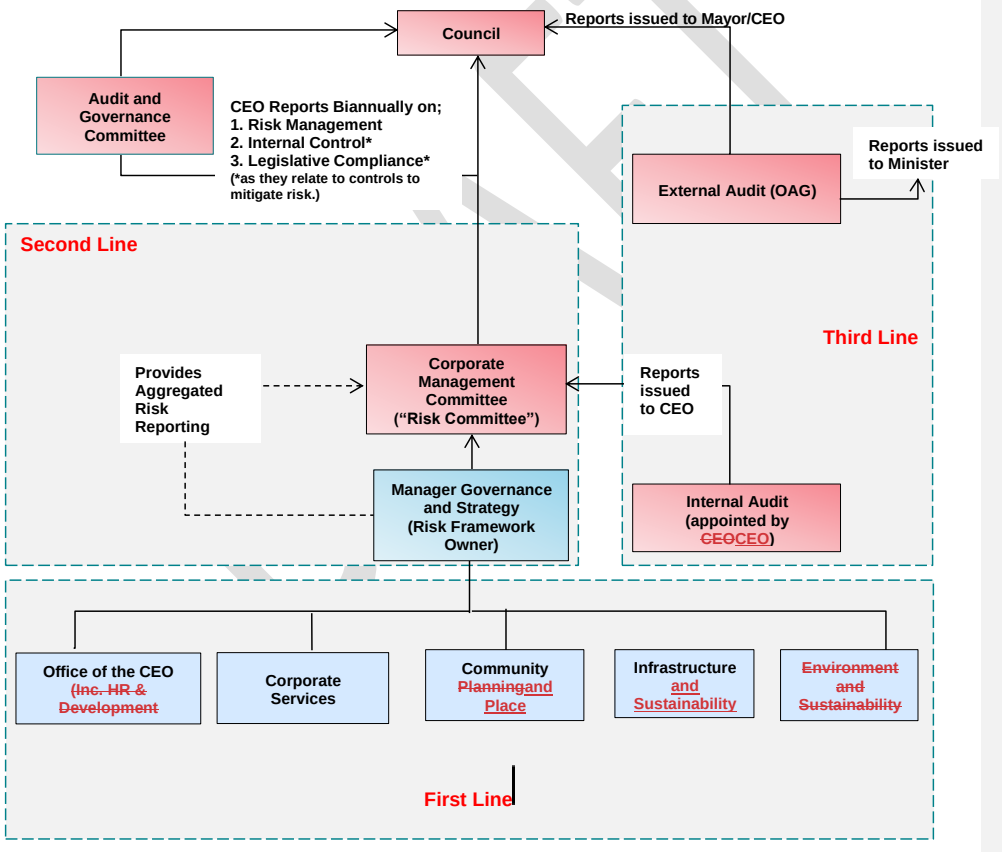
Internal audits and external audits are the **'3rd Line'** of defence, providing assurance to the Council, Audit and Governance Committee and Town Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the ~~CEO~~ CEO to report on the adequacy and effectiveness of internal control processes and procedures~~. The~~ with ~~scope of which would be determined by the CEO with input from the~~ the Audit and Governance Committee responsible for reviewing and recommending the approval of the internal Audit Plan and work program by Council.

External Audit – Appointed by the OAG to report independently on the annual financial statements.

Governance Structure

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



Roles & Responsibilities

Council

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

Audit and Governance Committee

- Support Council in providing effective corporate governance.
- Oversight of all matters that relate to the conduct of external and internal audits.
- Independent, objective and autonomous in deliberations.
- Recommendations to Council on Internal Auditor appointments following the RFQ process.

CEO / Corporate Management Committee

- Undertake internal Audits as required under *Local Government (Audit) Regulations 1996*.
- Liaise with Council in relation to risk acceptance requirements.
- Approve and review the appropriateness and effectiveness of the Risk Management Framework.
- Drive consistent embedding of a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk matters.
- Own and manage the Risk Profiles at Town Level.

Risk Framework Owner: Manager Governance and Strategy

- Oversee and facilitate the Risk Management Framework.
- Champion risk management within operational areas.
- Support reporting requirements for Risk matters.

Managers / Teams

- Drive risk management culture within work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Management Meetings, by incorporating the following agenda items:
    - New or emerging risks.
    - Review existing risks.
    - Control adequacy.
    - Outstanding issues and actions.

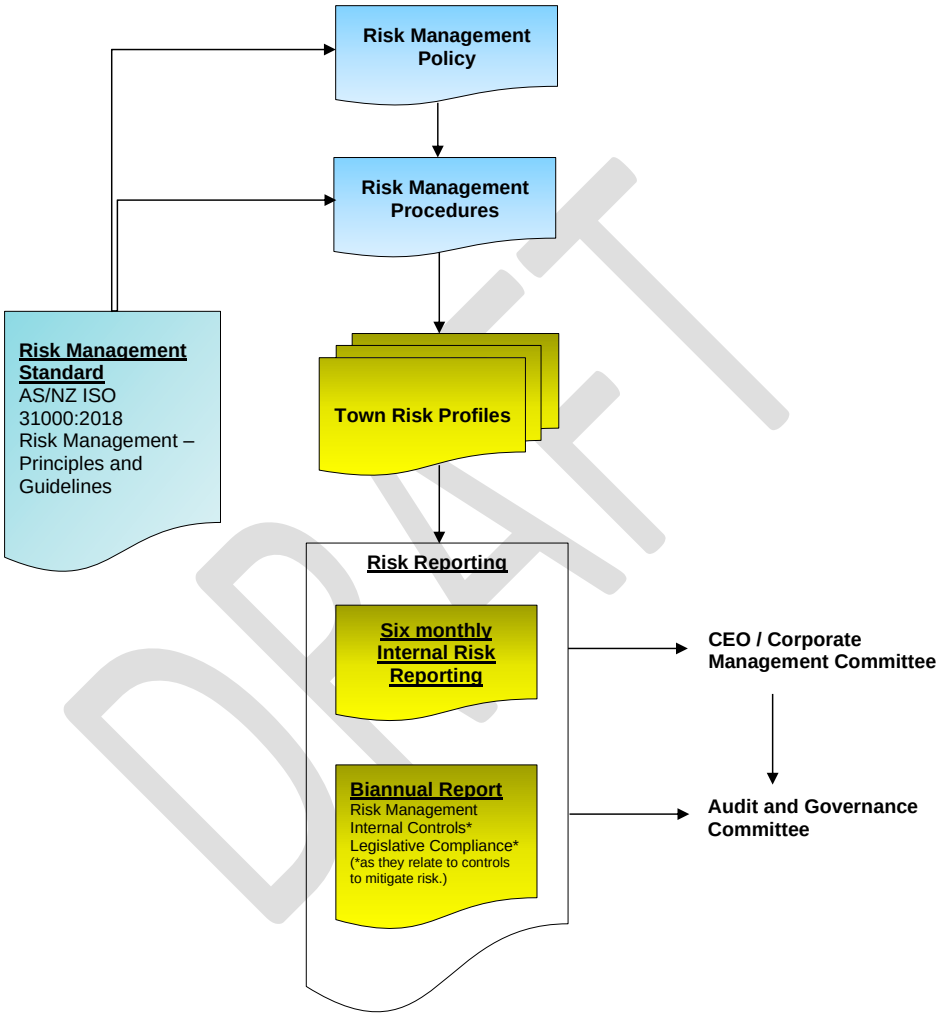
Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Document Structure (Framework)

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



Risk & Control Management

All Work Areas of the Town are required to assess and manage the Risk Profiles on an ongoing basis.

Each Manager, in conjunction with the Risk Framework Owner is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Town.
- Reviewed on at least a six monthly basis, 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 data inputs, workshops and ongoing business engagement.

Risk & Control Assessment

To ensure alignment with AS/NZ ISO 31000:2018 Risk Management, the following approach is to be adopted from a Risk & Control Assessment perspective:

A: Establishing the Context

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 Context

The Town's Risk Management Procedures provide the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed. In addition, existing Risk Themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Manager Governance and Strategy and CEO.

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.

Specific Risk Assessment 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.

For risk assessment purposes the Town has been divided into three levels of risk assessment context:

1. Strategic Context

This constitutes the Town's external environment and high-level direction. Inputs to establishing the strategic risk assessment environment may include:

- Organisation's Vision
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

2. 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 trying to be achieved. Note: these may already be documented in business plans, budgets, Service Level Plans etc.

3. 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 current or future 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

Using the specific risk assessment context as the foundation, and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

- What can go wrong? / What are areas of uncertainty? (Risk Description)
- How could 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)

C: Risk Analysis

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

- Based on the documented controls, analyse the risk in terms of Existing Control Ratings
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the risk rating (Level of Risk)

D: Risk Evaluation

The Town is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be documented and acceptable risks are then subject to the monitor and review process. Note: Individual Risks or Issues may need to be escalated due to urgency, level of risk or systemic nature.

E: Risk Treatment

For unacceptable risks, determine treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on:

- Cost versus benefit
- Ease of implementation
- Alignment to organisational values / objectives

Once a treatment has been fully implemented, the Manager Governance and Strategy 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: Monitoring & Review

The Town is to review all Risk Profiles at least on a six monthly basis or if triggered by one of the following:

- Changes to context,
- A treatment is implemented,
- An incident occurs or due to audit/regulator findings.

The Risk Framework Owner (~~RFO~~Manager Governance and Strategy) is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Corporate Management Committee will monitor significant risks and treatment implementation as part of their normal agenda item on a biannual basis with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Extreme
- Risks with Likelihood Rating of Almost Certain

The design and focus of the Risk Summary report will be determined from time to time on the direction of the CEO & Corporate Management Committee. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Town.

G: Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process. Council, through the Audit and Governance Committee will be provided with (biannual) update reports.

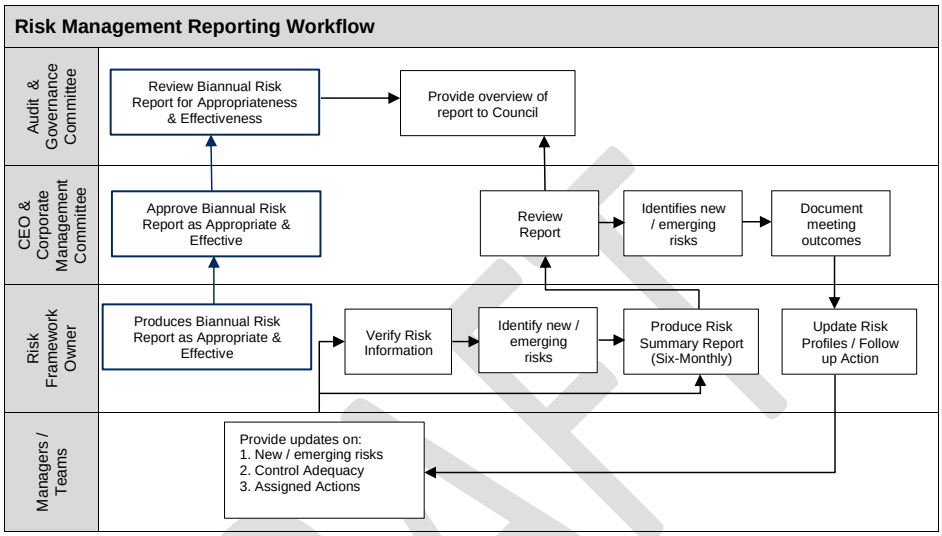
Risk management awareness and training will be provided to staff as part of their ~~OS&H~~WHS Program.

Risk management will be included within the employee induction process to ensure new employees are introduced to the Town's risk management culture.

Reporting Requirements

Coverage & Frequency

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 and emerging risks, control effectiveness and indicator performance to the Risk Framework Owner.
- Work through assigned actions and provide relevant updates to the Risk Framework Owner.
- Risks / Issues reported to the CEO & Corporate Management Committee are reflective of the current risk and control environment.

The Risk Framework Owner is responsible for:

- Ensuring Town Risk Profiles are formally reviewed and updated, at least on a six monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Producing a six-monthly Risk Report for the CEO & Corporate Management Committee which contains an overview Risk Summary for the Town.
- Annual Compliance Audit Return completion and lodgement.

Indicators

Indicators are required to be used for monitoring and validating risks and controls. The following describes the process for the creation and reporting of Indicators:

Identification

The following represent the minimum standards when identifying appropriate Indicator risks and controls:

- The risk description and casual factors are fully understood
- The Indicator is fully relevant to the risk or control
- Predictive Indicators are adopted wherever possible
- Indicators provide adequate coverage over monitoring 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 Indicator data is relevant to the risk or cControl.

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

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

Tolerances

Tolerances are set based on the Town's Risk Appetite. They may be set and agreed over three levels:

- Green – within appetite; no action required.
- Amber – the Indicator must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the Indicator must be escalated to the CEO & Corporate Management Committee where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & Review

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

When monitoring and reviewing Indicators, the overall trend should be considered over a longer timeframe than individual data movements. The trend of the 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 *outside* of the appetite framework is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria) for an extended period of time (generally 3 months or longer).

The following process is designed to provide a framework for those *outside* of the appetite framework identified risks.

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

- A description of the risk.
- 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.

Reasonable action should be taken to mitigate the risk. A lack of budget to remediate a material risk outside of appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (i.e. Corporate Management Committee)

Annual Controls Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Corporate Management Committee that sets out the control assurance activities to be conducted over the next 12 months. This plan needs to consider the following components.

- Coverage of all risk classes (~~Strategic, Operational~~Strategic, Operational and~~,~~ Project).
- Existing control adequacy ratings across the Town's Risk Profiles.
- Consider control coverage across a range of risk themes (where commonality exists).
- Building profiles around material controls to assist in design and operating effectiveness reviews.
- Consideration to significant incidents.
- Nature of operations.
- Additional or existing 2nd line assurance information / reviews (e.g. HR, Financial Services, IT).
- Frequency of monitoring / checks being performed.
- Review and development of Indicators.
- Timetable for assurance activities.
- Reporting requirements.

Whilst this document and subsequent actions are owned by the CEO, input and consultation will be sought from individual Work Areas.

Appendix A – Risk Assessment and Acceptance Criteria

MEASURES OF CONSEQUENCE

RATING	PEOPLE	INTERRUPTION TO SERVICE	REPUTATION (Social / Community)	COMPLIANCE	PROPERTY (Plant, Equipment, Buildings)	NATURAL ENVIRONMENT	FINANCIAL IMPACT
Insignificant (1)	Near-Miss	No material service interruption Less than 1 hour	Unsubstantiated, localised low impact on community trust, low profile or no media item.	No noticeable regulatory or statutory impact	Inconsequential damage.	Contained, reversible impact managed by on site response	Less than $105,000
Minor (2)	First Aid Treatment	Short term temporary interruption – backlog cleared < 1 day	Substantiated, localised impact on community trust or low media item	Some temporary non compliances	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response	$10,0010 - $50,000
Moderate (3)	Medical treatment / Lost time injury <30 Days	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Substantiated, public embarrassment, moderate impact on community trust or moderate media profile	Short term non-compliance but with significant regulatory requirements imposed	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies	$50,001 to $200,000
Major (4)	Lost time injury >30 Days / temporary disability	Prolonged interruption of services – additional resources; performance affected	Substantiated, public embarrassment, widespread high impact on community trust, high media profile, third party actions	Non-compliance results in termination of services or imposed penalties to Town / Officers	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies	$200 000-001 to $500,000
Extreme (5)	Fatality, permanent disability	Indeterminate prolonged interruption of services non- performance > 1 month	Substantiated, public embarrassment, widespread loss of community trust, hightrust, high widespread multiple media profile, third party actions	Non-compliance results in litigation, criminal charges or significant damages or penalties to Town / Officers	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact	>$500,000

Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt

MEASURES OF CONSEQUENCE (PROJECT)

LEVEL	RATING	Project TIME	Project COST	Project SCOPE / QUALITY
1	Insignificant	Exceeds deadline by >5% of project timeline	Exceeds project budget by 2%	Minor variations to project scope or quality
2	Minor	Exceeds deadline by >10% of project timeline	Exceeds project budget by 5%	Scope creep requiring additional work, time or resources. Reduced perception of quality by Stakeholders.
3	Moderate	Exceeds deadline by >15% of project timeline	Exceeds project budget by 7.5%	Scope creep requiring additional work, time and resources or shortcuts being taken. Stakeholder concerns.
4	Major	Exceeds deadline by >20% of project timeline	Exceeds project budget by 15%	Project goals, deliverables, costs and/or deadline failures. Project no longer aligned with the project scope Stakeholder intervention in project.
5	Extreme	Exceeds deadline by 25% of project timeline	Exceeds project budget by 20%	Failure to meet project objectives. Project outcomes negatively affecting the community or the environment. Public embarrassment, third party actions.

MEASURES OF LIKELIHOOD

Level	Rating	Description	Frequency
5	**Almost Certain**	The event is expected to occur in most circumstances	More than once per year
4	**Likely**	The event will probably occur in most circumstances	At least once per year
3	**Possible**	The event should occur at some time	At least once in 3 years
2	**Unlikely**	The event could occur at some time	At least once in 10 years
1	**Rare**	The event may only occur in exceptional circumstances	Less than once in 15 years

Formatted: Font: 9 pt
Formatted Table
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt

RISK MATRIX

Consequence / Likelihood		Insignificant	Minor	Moderate	Major	Extreme
		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)

Formatted Table

RISK ACCEPTANCE

Risk Rank	Description	Criteria	Responsibility
LOW (1-4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MEDIUM (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Corporate Management Committee
EXTREME (17-25)	Unacceptable	Risk only acceptable with excellent 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

Town of Bassendean Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
Effective	There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

Formatted Table

Appendix B – Risk Profile Template

Risk Theme	**Date**
(What could go right / wrong?) *Definition of Theme*	

Potential causes *(What could cause it to go right / wrong?)*
List of potential causes

Controls ***(What we have in place to prevent it going wrong)***	**Type**	**Date**	**Town Rating**
List of Controls			

Overall Control Ratings:	

Consequence Category	**Risk Ratings**	**Town Rating**
	Consequence:	
	Likelihood:	
	Overall Risk Ratings:	

Indicators ***(These would 'indicate' to us that something has gone right / wrong)***	**Tolerance**	**Date**	**Overall Town Result**
List of Indicators			
Comments *Rationale for all above ratings*			

Current Issues / Actions / Treatments	**Due Date**	**Responsibility**
List current issues / actions / treatments		

Appendix C – Risk Theme Definitions

1. **Asset Sustainability practices**

➢ Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and ultimate disposal. Areas included in the scope are:

- Inadequate design (not fit for purpose).
- Ineffective usage (down time).
- Outputs not meeting expectations.
- Inadequate maintenance activities.
- Inadequate financial management and planning.

It does not include issues with the inappropriate use of the Plant, Equipment or Machinery. Refer Misconduct.

2. **Business & Community disruption**

➢ Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal Town business activities. The event may result in damage to buildings, property, plant & equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (incl vandalism). This includes:

- Lack of (or inadequate) emergency response / business continuity plans.
- Lack of training to specific individuals or availability of appropriate emergency response.
- Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.
- Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc

This does not include disruptions due to IT Systems or infrastructure related failures - refer "Failure of IT & communication systems and infrastructure".

3. **Failure to fulfil Compliance requirements**

➢ Failures to correctly identify, interpret, assess, respond and communicate laws and regulations as a result of an inadequate compliance framework. This could result in fines, penalties, litigation or increase scrutiny from regulators or agencies. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated legal documentation (internal & public domain) to reflect changes.

This does not include ~~Occupational Safety & Health~~*Work Health and Safety Act 2020* (refer "Inadequate safety and security practices") or any Employment Practices based legislation (refer "Ineffective Employment practices).

Formatted: Font: Italic

It does include the *Local Government Act 1995*, *Health Act 1911*, *Building Act 2011*, *Privacy Act 1988* and all other legislative based obligations for Local Government.

Formatted: Font: Italic

4. **Document Management Processes**

➢ Failure to adequately capture, store, archive, retrieve, provision and / or disposal of documentation. This includes:

- Contact lists.
- Procedural documents.
- 'Application' proposals/documents.
- Contracts.
- Forms, requests or other documents.

5. **Employment practices**

➢ Failure to effectively manage and lead human resources (full/part time, casuals, temporary and volunteers). This includes not having an effective Human Resources Framework in addition to not

having appropriately qualified or experienced people in the right roles or not having sufficient staff numbers to achieve objectives. ~~-~~Other areas in this risk theme to consider are~~:~~:

- Breaching employee regulations (excluding ~~OH&~~WH~~S~~S).
- Discrimination, Harassment & Bullying in the workplace.
- Poor employee wellbeing (causing stress).
- Key person dependencies without effective succession planning in place.
- Induction issues.
- Terminations (including any tribunal issues).
- Industrial activity.

Care should be taken when considering insufficient staff numbers as the underlying issue could be process inefficiencies.

6. Engagement practices

- Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or ~~Elected~~ Council Members. ~~-~~This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. ~~-~~For example~~:~~:

  - Following up on any access & inclusion issues.
  - Infrastructure Projects.
  - Regional or District Committee attendance.
  - Local Planning initiatives.
  - ~~Strategic~~ Council Planning initiatives.

This does not include instances whereby Community expectations have not been met for standard service provisions such as Community Events, Library Services and / or Bus/Transport services.

7. Environment management.

- Inadequate prevention, identification, enforcement and management of environmental issues.

The scope includes~~:~~:

- Lack of adequate planning and management of ~~coastal~~ waterway erosion issues.
- Failure to identify and effectively manage contaminated sites (including groundwater usage).
- Waste ~~facilities (landfill / transfer stations).~~ services.
- Weed control.
- Ineffective management of water sources (reclaimed, potable).
- Illegal dumping / Illegal clearing / Illegal land use.

8. Errors, Omissions, Delays

- Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process. This includes instances of~~:~~:

  - Human errors, incorrect or incomplete processing.
  - Inaccurate recording, maintenance, testing and / or reconciliation of data.
  - Errors or inadequacies in model methodology, design, calculation or implementation of models.

This may result in incomplete or inaccurate information. ~~-~~Consequences include~~:~~:

- Inaccurate data being used for management decision making and reporting.
- Delays in service to customers.
- Inaccurate data provided to customers.

This excludes process failures caused by inadequate / incomplete procedural documentation - refer “Inadequate Document Management Processes”.

9. External theft & fraud (incl Cyber Crime)

- Loss of funds, assets, data or unauthorised access, (whether attempts or successful) by external parties, through any means (including electronic), for the purposes of:

  - Fraud – benefit or gain by deceit.
  - Malicious Damage – hacking, deleting, breaking or reducing the integrity or performance of systems.
  - Theft – stealing of data, assets or information (no deceit).

Examples include:

- Scam Invoices.
- Cash or other valuables from 'Outstations'.

10. Management of Facilities / Venues / Events

- Failure to effectively manage the day to day operations of facilities and / or venues.

This includes:

- Inadequate procedures in place to manage the quality or availability.
- Ineffective signage.
- Booking issues.
- Financial interactions with hirers / users.
- Oversight / provision of peripheral services (e.g. cleaning / maintenance).

11. IT & Communications Systems and Infrastructure

- Instability, degradation of performance, or other failure of IT Systems, Infrastructure, Communication or Utility causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked. Examples include failures or disruptions caused by:

  - Hardware and/or Software.
  - IT Network.
  - Failures of IT Vendors.

This also includes where poor governance results in the breakdown of IT maintenance such as:

- Configuration management.
- Performance Monitoring.
- IT Incident, Problem Management & Disaster Recovery Processes.

This does not include new system implementations - refer "Inadequate Project / Change Management".

12. Misconduct

- Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority. This would include instances of:

  - Relevant authorisations not obtained.
  - Distributing confidential information.
  - Accessing systems and / or applications without correct authority to do so.
  - Misrepresenting data in reports.
  - Theft by an employee
  - Collusion between Internal & External parties

This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays, or Inaccurate Advice / Information.

13. **Project / Cehange Management**

- Inadequate analysis, design, delivery and / or status reporting of change initiatives, resulting in additional expenses, time requirements or scope changes. This includes:
  - Inadequate Change Management Framework to manage and monitor change activities.
  - Inadequate understanding of the impact of project change on the business.
  - Failures in the transition of projects into standard operations.
  - Failure to implement new systems.
  - Failures of IT Project Vendors/Contractors.

14. **Safety and Security practices**

- Non-compliance with the ~~Occupation Safety & Health Act~~*Work Health and Safety Act 2020*, associated regulations and standards. It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are:
  - Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants.
  - Inadequate Organisational Emergency Management requirements (evacuation diagrams, drills, wardens etc).
  - Inadequate security protection measures in place for buildings, depots and other places of work (vehicle, community etc).
  - Public Liability Claims, due to negligence or personal injury.
  - Employee Liability Claims due to negligence or personal injury.
  - Inadequate or unsafe modifications to plant & equipment.

15. **Supplier / Contract Management**

- Inadequate management of external Suppliers, Contractors, IT Vendors or Consultants engaged for core operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes. This also includes:
  - Concentration issues.
  - Vendor sustainability.

Formatted: Font: Italic

Town of Bassendean

Risk Management Framework

- Risk Management Policy
- Risk Management Procedures

CONFIDENTIAL

September 2024

Version: 2.0

Table of Contents

VERSION CONTROL			
Number	**Date**	**Item**	**Reason**
1	15/12/2022	Measures of Consequence Table	Amended measures of consequence table financial impact at minor amended from $10,000 - $50,000, to $15,001 - $50,000'. Major amended from $200,000 to $500,000' to '$200,001 to $500,000'.
2	04/09/2024	Administrative Review	Amended 'elected members' to Council Members for contemporary reference. Minor administrative amendments to organisational structure and process charts throughout.
3			
4			
5			
6			
7			

Introduction

The Policy and Procedures form the Risk Management Framework for the Town of Bassendean ("the Town"). 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 Australia/New Zealand Standard ISO 31000:2018 Risk Management – Principles and 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 along with existing time, resource and workload pressures.

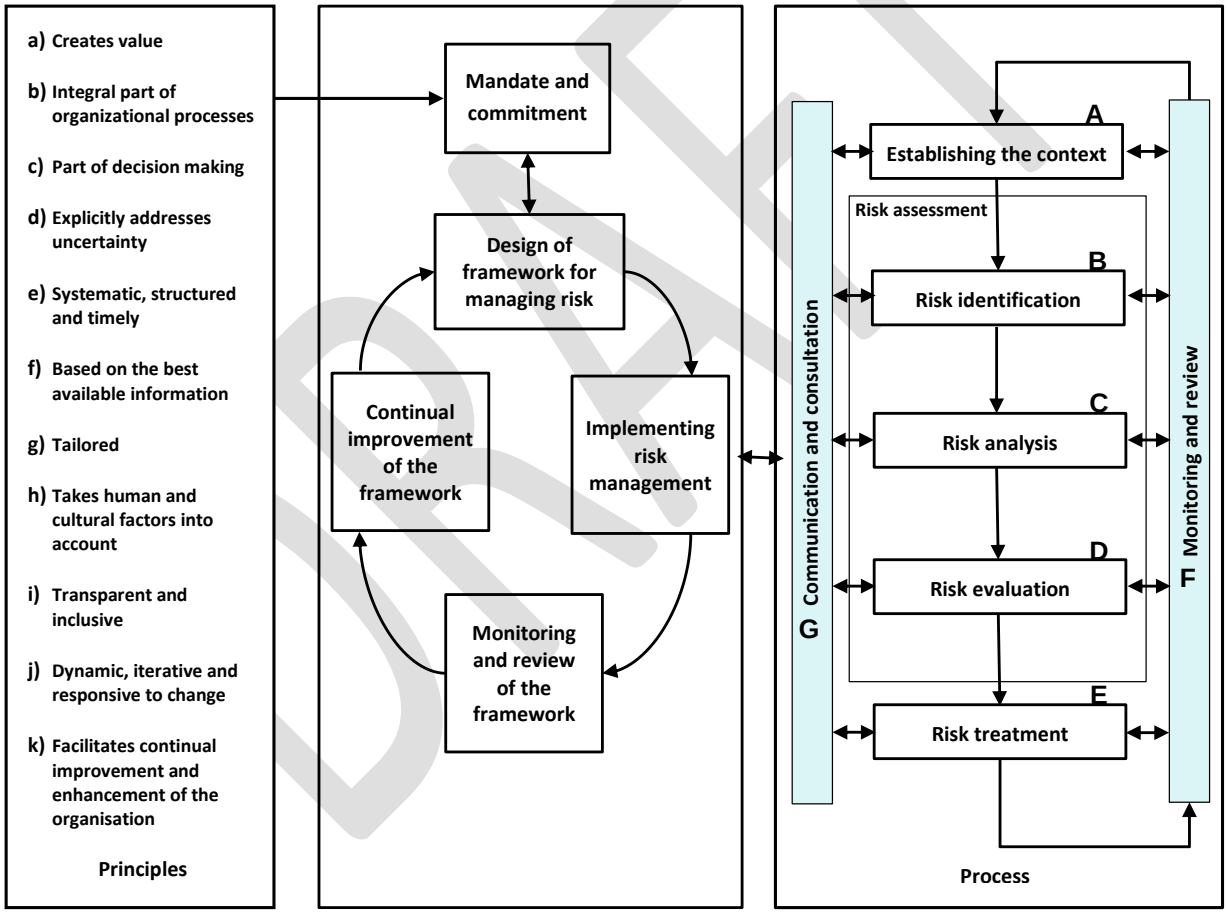


Figure 1: Risk Management Process (Source: AS/NZS 31000:2018)

Risk Management Policy

Purpose

The Town of Bassendean's ("the Town") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Town's strategies, goals or objectives.

Policy Scope

This policy applies to all of the Town's activities and decision making and applies to all Council Members, employees, contractors and volunteers. The policy provides a framework for the Town's strategic, operational and project risks.

Policy Statement

It is the Town's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2018 Risk management), in the management of all risks that may affect the Town, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Town's Integrated Planning Framework.

The Town's Corporate Management Committee will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee, Council Member, volunteer and contractor within the Town is recognised as having a role in risk management.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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 the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.

- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Town defined its risk appetite through the development and endorsement of the Town's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All strategic risks to be reported at a corporate level are to be assessed according to the Town's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Corporate Management Committee.

Roles, Responsibilities & Accountabilities

Council's role is to:

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town will implement and integrate a monitor and review process to report on the achievement of the Risk Management objectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be kept under review by the Town's Corporate Management Committee and will be formally reviewed by Council biennially.

Document Control box			
Document Responsibilities:			
Owner:	Chief Executive Officer	**Owner Business Unit:**	Office of the Chief Executive Officer
Inception Date:	OCM 22/03/2022	**Decision Maker:**	Council
Review Date:	Biennial	**Repeal and Replace:**	N/A
Review Frequency	September 2026		
Compliance Requirements:			
Legislation:	***Local Government Act 1995***		

Risk Management Procedures

Governance

Appropriate governance of risk management within the Town of Bassendean (the "Town") provides:

- Transparency of decision making.
- Clear identification of the roles and responsibilities of 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 biennially.

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 the delivery of Strategic and 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 decision-making process of risk.
- Prepare risk acceptance proposals where necessary, based on level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Town's Risk Framework Owner (Manager Governance and Strategy) acts as the primary **'2nd Line'**. This position owns and manages the framework for risk management, drafts and implements governance procedures and provides the necessary tools and training to support the 1st line process. The Corporate Management Committee supplements the second line of defence.

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 & Corporate Management Committee and the Audit and Governance Committee.

Third Line of Defence

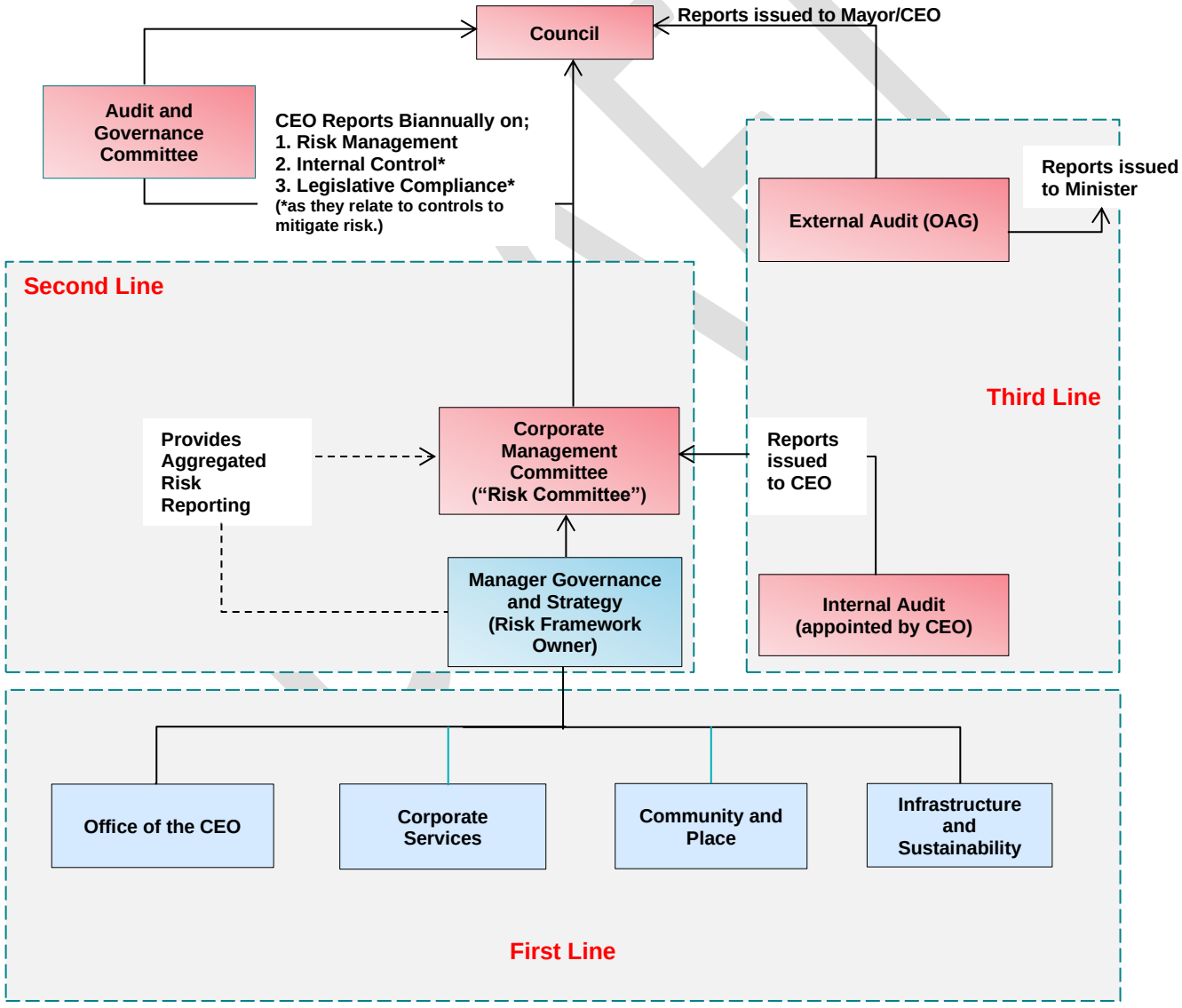
Internal audits and external audits are the **'3rd Line'** of defence, providing assurance to the Council, Audit and Governance Committee and Town Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures with the Audit and Governance Committee responsible for reviewing and recommending the approval of the Internal Audit Plan and Work Program by Council

External Audit – Appointed by the OAG to report independently on the annual financial statements.

Governance Structure

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



Roles & Responsibilities

Council

- Review and approve the Town's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Establish and maintain an Audit and Governance Committee in terms of the *Local Government Act 1995*.

Audit and Governance Committee

- Support Council in providing effective corporate governance.
- Oversight of all matters that relate to the conduct of external and internal audits.
- Independent, objective and autonomous in deliberations.
- Recommendations to Council on Internal Auditor appointments following the RFQ process.

CEO / Corporate Management Committee

- Undertake internal Audits as required under *Local Government (Audit) Regulations 1996.*
- Liaise with Council in relation to risk acceptance requirements.
- Approve and review the appropriateness and effectiveness of the Risk Management Framework.
- Drive consistent embedding of a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk matters.
- Own and manage the Risk Profiles at Town Level.

Risk Framework Owner: Manager Governance and Strategy

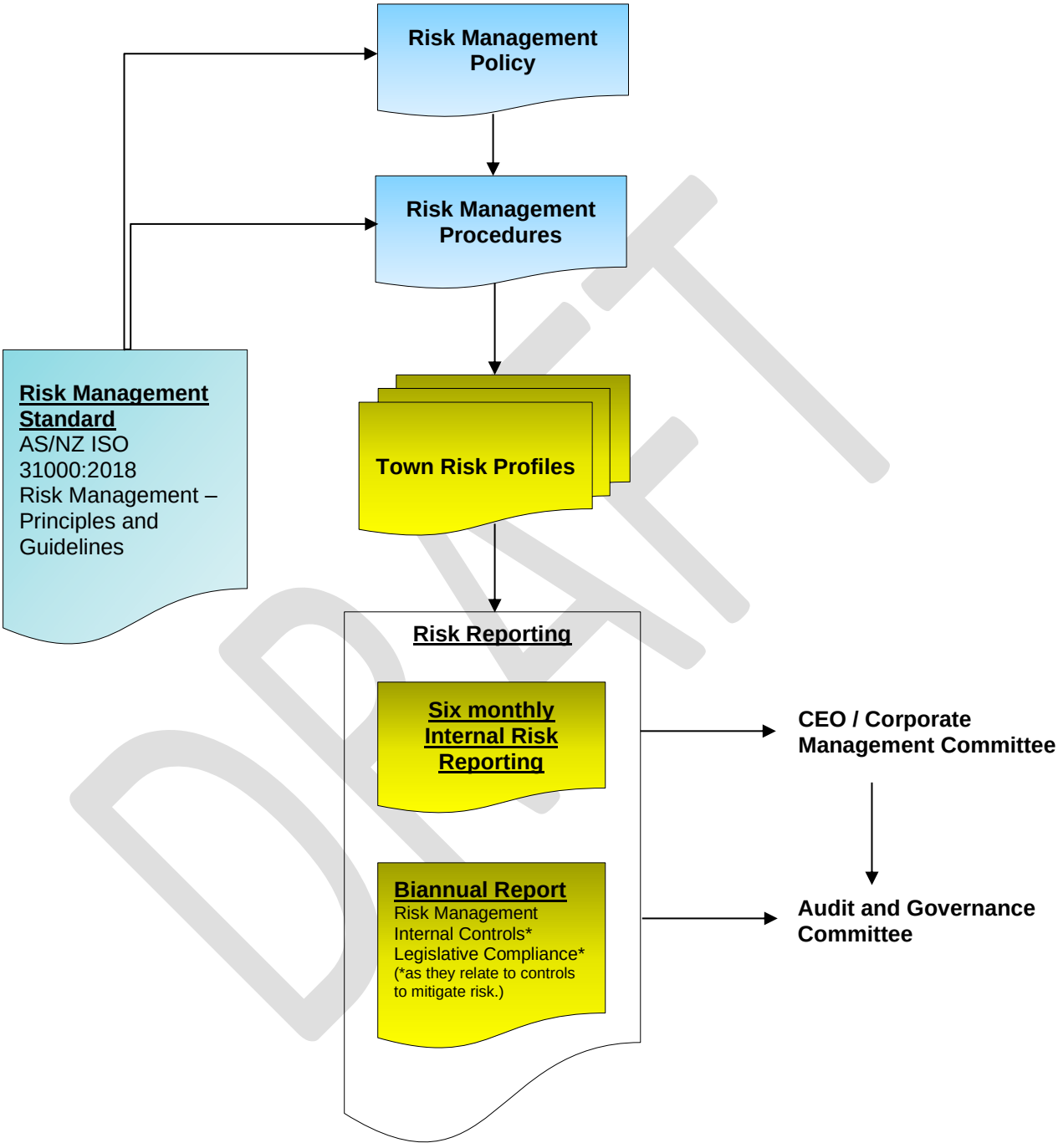
- Oversee and facilitate the Risk Management Framework.
- Champion risk management within operational areas.
- Support reporting requirements for Risk matters.

Managers / Teams

- Drive risk management culture within work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Management Meetings, by incorporating the following agenda items:
    - New or emerging risks.
    - Review existing risks.
    - Control adequacy.
    - Outstanding issues and actions.

Document Structure (Framework)

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



Risk & Control Management

All Work Areas of the Town are required to assess and manage the Risk Profiles on an ongoing basis.

Each Manager, in conjunction with the Risk Framework Owner is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Town.
- Reviewed on at least a six monthly basis, 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 data inputs, workshops and ongoing business engagement.

Risk & Control Assessment

To ensure alignment with AS/NZ ISO 31000:2018 Risk Management, the following approach is to be adopted from a Risk & Control Assessment perspective:

A: Establishing the Context

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 Context

The Town's Risk Management Procedures provide the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed. In addition, existing Risk Themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Manager Governance and Strategy and CEO.

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.

Specific Risk Assessment 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.

For risk assessment purposes the Town has been divided into three levels of risk assessment context:

1. Strategic Context

This constitutes the Town's external environment and high-level direction. Inputs to establishing the strategic risk assessment environment may include:

- Organisation's Vision
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

2. 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 trying to be achieved. Note: these may already be documented in business plans, budgets, Service Level Plans etc.

3. 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 current or future 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

Using the specific risk assessment context as the foundation, and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

- What can go wrong? / What are areas of uncertainty? (Risk Description)
- How could 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)

C: Risk Analysis

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

- Based on the documented controls, analyse the risk in terms of Existing Control Ratings
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the risk rating (Level of Risk)

D: Risk Evaluation

The Town is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be documented and acceptable risks are then subject to the monitor and review process. Note: Individual Risks or Issues may need to be escalated due to urgency, level of risk or systemic nature.

E: Risk Treatment

For unacceptable risks, determine treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on:

- Cost versus benefit
- Ease of implementation
- Alignment to organisational values / objectives

Once a treatment has been fully implemented, the Manager Governance and Strategy 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: Monitoring & Review

The Town is to review all Risk Profiles at least on a six monthly basis or if triggered by one of the following:

- Changes to context.
- A treatment is implemented.
- An incident occurs or due to audit/regulator findings.

The Risk Framework Owner (Manager Governance and Strategy) is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Corporate Management Committee will monitor significant risks and treatment implementation as part of their normal agenda item on a biannual basis with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Extreme
- Risks with Likelihood Rating of Almost Certain

The design and focus of the Risk Summary report will be determined from time to time on the direction of the CEO & Corporate Management Committee. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Town.

G: Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process. Council, through the Audit and Governance Committee will be provided with (biannual) update reports.

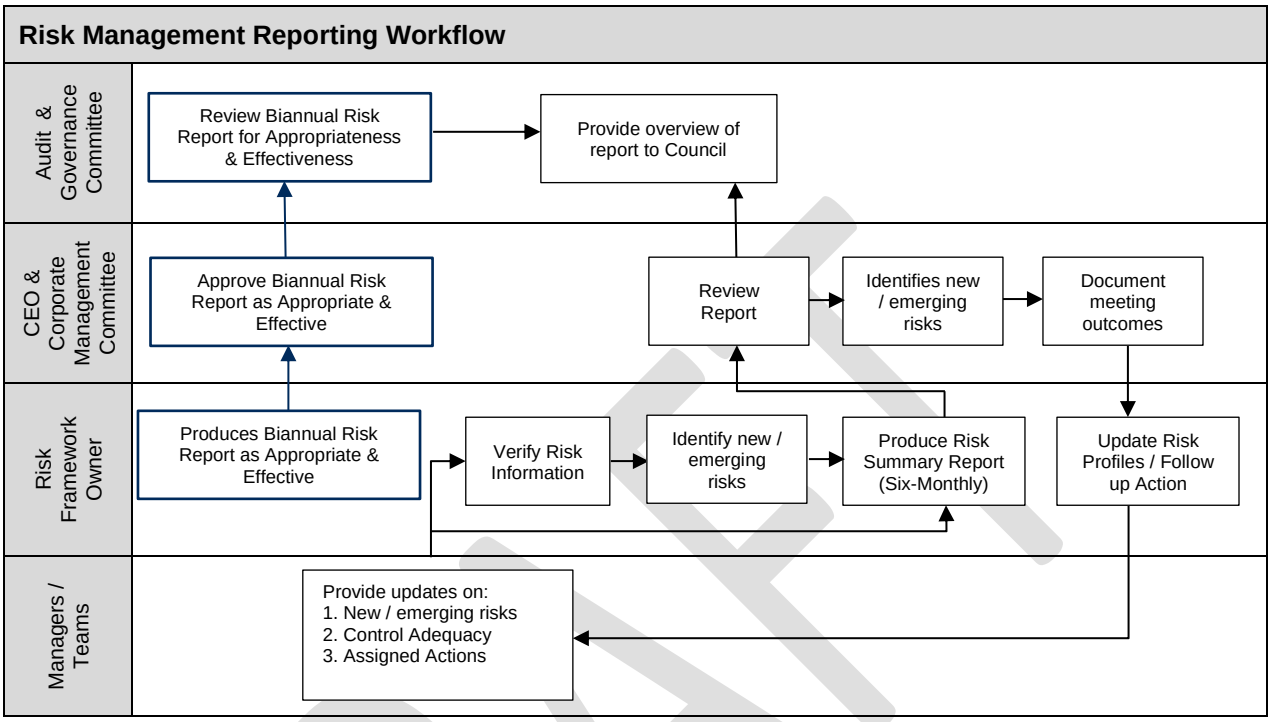
Risk management awareness and training will be provided to staff as part of their WHS Program.

Risk management will be included within the employee induction process to ensure new employees are introduced to the Town's risk management culture.

Reporting Requirements

Coverage & Frequency

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 and emerging risks, control effectiveness and indicator performance to the Risk Framework Owner.
- Work through assigned actions and provide relevant updates to the Risk Framework Owner.
- Risks / Issues reported to the CEO & Corporate Management Committee are reflective of the current risk and control environment.

The Risk Framework Owner is responsible for:

- Ensuring Town Risk Profiles are formally reviewed and updated, at least on a six monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Producing a six-monthly Risk Report for the CEO & Corporate Management Committee which contains an overview Risk Summary for the Town.
- Annual Compliance Audit Return completion and lodgement.

Indicators

Indicators are required to be used for monitoring and validating risks and controls. The following describes the process for the creation and reporting of Indicators:

Identification

The following represent the minimum standards when identifying appropriate Indicator risks and controls:

- The risk description and casual factors are fully understood
- The Indicator is fully relevant to the risk or control
- Predictive Indicators are adopted wherever possible
- Indicators provide adequate coverage over monitoring 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 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 Indicators can be used to provide a level of assurance on data integrity.

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

Tolerances

Tolerances are set based on the Town's Risk Appetite. They may be set and agreed over three levels:

- Green – within appetite; no action required.
- Amber – the Indicator must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the Indicator must be escalated to the CEO & Corporate Management Committee where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & Review

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

When monitoring and reviewing Indicators, the overall trend should be considered over a longer timeframe than individual data movements. The trend of the 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 *outside* of the appetite framework is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria) for an extended period of time (generally 3 months or longer).

The following process is designed to provide a framework for those *outside* of the appetite framework identified risks.

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

- A description of the risk.
- 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.

Reasonable action should be taken to mitigate the risk. A lack of budget to remediate a material risk outside of appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (i.e. Corporate Management Committee)

Annual Controls Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Corporate Management Committee that sets out the control assurance activities to be conducted over the next 12 months. This plan needs to consider the following components.

- Coverage of all risk classes (Strategic, Operational andProject).
- Existing control adequacy ratings across the Town's Risk Profiles.
- Consider control coverage across a range of risk themes (where commonality exists).
- Building profiles around material controls to assist in design and operating effectiveness reviews.
- Consideration to significant incidents.
- Nature of operations.
- Additional or existing 2nd line assurance information / reviews (e.g. HR, Financial Services, IT).
- Frequency of monitoring / checks being performed.
- Review and development of Indicators.
- Timetable for assurance activities.
- Reporting requirements.

Whilst this document and subsequent actions are owned by the CEO, input and consultation will be sought from individual Work Areas.

Appendix A – Risk Assessment and Acceptance Criteria

MEASURES OF CONSEQUENCE

RATING	PEOPLE	INTERRUPTION TO SERVICE	REPUTATION (Social / Community)	COMPLIANCE	PROPERTY (Plant, Equipment, Buildings)	NATURAL ENVIRONMENT	FINANCIAL IMPACT
Insignificant (1)	Near-Miss	No material service interruption Less than 1 hour	Unsubstantiated, localised low impact on community trust, low profile or no media item.	No noticeable regulatory or statutory impact	Inconsequential damage.	Contained, reversible impact managed by on site response	Less than $10,000
Minor (2)	First Aid Treatment	Short term temporary interruption – backlog cleared < 1 day	Substantiated, localised impact on community trust or low media item	Some temporary non compliances	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response	$10,001 - $50,000
Moderate (3)	Medical treatment / Lost time injury <30 Days	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Substantiated, public embarrassment, moderate impact on community trust or moderate media profile	Short term non-compliance but with significant regulatory requirements imposed	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies	$50,001 to $200,000
Major (4)	Lost time injury >30 Days / temporary disability	Prolonged interruption of services – additional resources; performance affected	Substantiated, public embarrassment, widespread high impact on community trust, high media profile, third party actions	Non-compliance results in termination of services or imposed penalties to Town / Officers	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies	$200 001 to $500,000
Extreme (5)	Fatality, permanent disability	Indeterminate prolonged interruption of services non- performance > 1 month	Substantiated, public embarrassment, widespread loss of community trust, high widespread multiple media profile, third party actions	Non-compliance results in litigation, criminal charges or significant damages or penalties to Town / Officers	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact	>$500,000

MEASURES OF CONSEQUENCE (PROJECT)

LEVEL	RATING	Project TIME	Project COST	Project SCOPE / QUALITY
1	**Insignificant**	Exceeds deadline by >5% of project timeline	Exceeds project budget by 2%	Minor variations to project scope or quality
2	**Minor**	Exceeds deadline by >10% of project timeline	Exceeds project budget by 5%	Scope creep requiring additional work, time or resources. Reduced perception of quality by Stakeholders.
3	**Moderate**	Exceeds deadline by >15% of project timeline	Exceeds project budget by 7.5%	Scope creep requiring additional work, time and resources or shortcuts being taken. Stakeholder concerns.
4	**Major**	Exceeds deadline by >20% of project timeline	Exceeds project budget by 15%	Project goals, deliverables, costs and/or deadline failures. Project no longer aligned with the project scope Stakeholder intervention in project.
5	**Extreme**	Exceeds deadline by 25% of project timeline	Exceeds project budget by 20%	Failure to meet project objectives. Project outcomes negatively affecting the community or the environment. Public embarrassment, third party actions.

MEASURES OF LIKELIHOOD

Level	Rating	Description	Frequency
5	**Almost Certain**	The event is expected to occur in most circumstances	More than once per year
4	**Likely**	The event will probably occur in most circumstances	At least once per year
3	**Possible**	The event should occur at some time	At least once in 3 years
2	**Unlikely**	The event could occur at some time	At least once in 10 years
1	**Rare**	The event may only occur in exceptional circumstances	Less than once in 15 years

RISK MATRIX

Consequence / Likelihood		Insignificant	Minor	Moderate	Major	Extreme
		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

Risk Rank	Description	Criteria	Responsibility
LOW (1-4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MEDIUM (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Corporate Management Committee
EXTREME (17-25)	Unacceptable	Risk only acceptable with excellent 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

Town of Bassendean Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
Effective	There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

Appendix B – Risk Profile Template

Risk Theme	Date
(What could go right / wrong?) *Definition of Theme*	

Potential causes *(What could cause it to go right / wrong?)*
List of potential causes

Controls ***(What we have in place to prevent it going wrong)***	**Type**	**Date**	**Town Rating**
List of Controls			

Overall Control Ratings:	

Consequence Category	**Risk Ratings**	**Town Rating**
	Consequence:	
	Likelihood:	

Overall Risk Ratings:	

Indicators ***(These would 'indicate' to us that something has gone right / wrong)***	**Tolerance**	**Date**	**Overall Town Result**
List of Indicators			
Comments *Rationale for all above ratings*			

Current Issues / Actions / Treatments	**Due Date**	**Responsibility**
List current issues / actions / treatments		

Appendix C – Risk Theme Definitions

1. Asset Sustainability practices

- Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and ultimate disposal. Areas included in the scope are:
  - Inadequate design (not fit for purpose).
  - Ineffective usage (down time).
  - Outputs not meeting expectations.
  - Inadequate maintenance activities.
  - Inadequate financial management and planning.

It does not include issues with the inappropriate use of the Plant, Equipment or Machinery. Refer Misconduct.

2. Business & Community disruption

- Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal Town business activities. The event may result in damage to buildings, property, plant & equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (incl vandalism). This includes:
  - Lack of (or inadequate) emergency response / business continuity plans.
  - Lack of training to specific individuals or availability of appropriate emergency response.
  - Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.
  - Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc

This does not include disruptions due to IT Systems or infrastructure related failures - refer "Failure of IT & communication systems and infrastructure".

3. Failure to fulfil Compliance requirements

- Failures to correctly identify, interpret, assess, respond and communicate laws and regulations as a result of an inadequate compliance framework. This could result in fines, penalties, litigation or increase scrutiny from regulators or agencies. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated legal documentation (internal & public domain) to reflect changes.

This does not include *Work Health and Safety Act 2020* (refer "Inadequate safety and security practices") or any Employment Practices based legislation (refer “Ineffective Employment practices).

It does include the *Local Government Act 1995, Health Act 1911, Building Act 2011, Privacy Act 1988* and all other legislative based obligations for Local Government.

4. Document Management Processes

- Failure to adequately capture, store, archive, retrieve, provision and / or disposal of documentation. This includes:
  - Contact lists.
  - Procedural documents.
  - 'Application' proposals/documents.
  - Contracts.
  - Forms, requests or other documents.

5. Employment practices

- Failure to effectively manage and lead human resources (full/part time, casuals, temporary and volunteers). This includes not having an effective Human Resources Framework in addition to not

having appropriately qualified or experienced people in the right roles or not having sufficient staff numbers to achieve objectives. Other areas in this risk theme to consider are:

- Breaching employee regulations (excluding WHS).
- Discrimination, Harassment & Bullying in the workplace.
- Poor employee wellbeing (causing stress).
- Key person dependencies without effective succession planning in place.
- Induction issues.
- Terminations (including any tribunal issues).
- Industrial activity.

Care should be taken when considering insufficient staff numbers as the underlying issue could be process inefficiencies.

6. Engagement practices

➢ Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or Council Members. This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. For example:

- Following up on any access & inclusion issues.
- Infrastructure Projects.
- Regional or District Committee attendance.
- Local Planning initiatives.
- Council Planning initiatives.

This does not include instances whereby Community expectations have not been met for standard service provisions such as Community Events, Library Services and / or Bus/Transport services.

7. Environment management.

➢ Inadequate prevention, identification, enforcement and management of environmental issues.

The scope includes:

- Lack of adequate planning and management of waterway erosion issues.
- Failure to identify and effectively manage contaminated sites (including groundwater usage).
- Waste services.
- Weed control.
- Ineffective management of water sources (reclaimed, potable).
- Illegal dumping / Illegal clearing / Illegal land use.

8. Errors, Omissions, Delays

➢ Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process. This includes instances of:

- Human errors, incorrect or incomplete processing.
- Inaccurate recording, maintenance, testing and / or reconciliation of data.
- Errors or inadequacies in model methodology, design, calculation or implementation of models.

This may result in incomplete or inaccurate information. Consequences include:

- Inaccurate data being used for management decision making and reporting.
- Delays in service to customers.
- Inaccurate data provided to customers.

This excludes process failures caused by inadequate / incomplete procedural documentation - refer “Inadequate Document Management Processes”.

9. External theft & fraud (incl Cyber Crime)

➢ Loss of funds, assets, data or unauthorised access, (whether attempts or successful) by external parties, through any means (including electronic), for the purposes of:

- Fraud – benefit or gain by deceit.
- Malicious Damage – hacking, deleting, breaking or reducing the integrity or performance of systems.
- Theft – stealing of data, assets or information (no deceit).

Examples include:

- Scam Invoices.
- Cash or other valuables from 'Outstations'.

10. Management of Facilities / Venues / Events

➢ Failure to effectively manage the day to day operations of facilities and / or venues.

This includes:

- Inadequate procedures in place to manage the quality or availability.
- Ineffective signage.
- Booking issues.
- Financial interactions with hirers / users.
- Oversight / provision of peripheral services (e.g. cleaning / maintenance).

11. IT & Communications Systems and Infrastructure

➢ Instability, degradation of performance, or other failure of IT Systems, Infrastructure, Communication or Utility causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked. Examples include failures or disruptions caused by:

- Hardware and/or Software.
- IT Network.
- Failures of IT Vendors.

This also includes where poor governance results in the breakdown of IT maintenance such as:

- Configuration management.
- Performance Monitoring.
- IT Incident, Problem Management & Disaster Recovery Processes.

This does not include new system implementations - refer "Inadequate Project / Change Management".

12. Misconduct

➢ Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority. This would include instances of:

- Relevant authorisations not obtained.
- Distributing confidential information.
- Accessing systems and / or applications without correct authority to do so.
- Misrepresenting data in reports.
- Theft by an employee
- Collusion between Internal & External parties

This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays, or Inaccurate Advice / Information.

13. Project / Change Management

- Inadequate analysis, design, delivery and / or status reporting of change initiatives, resulting in additional expenses, time requirements or scope changes. This includes:

  - Inadequate Change Management Framework to manage and monitor change activities.
  - Inadequate understanding of the impact of project change on the business.
  - Failures in the transition of projects into standard operations.
  - Failure to implement new systems.
  - Failures of IT Project Vendors/Contractors.

14. Safety and Security practices

- Non-compliance with the *Work Health and Safety Act 2020*, associated regulations and standards. It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are:

  - Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants.
  - Inadequate Organisational Emergency Management requirements (evacuation diagrams, drills, wardens etc).
  - Inadequate security protection measures in place for buildings, depots and other places of work (vehicle, community etc).
  - Public Liability Claims, due to negligence or personal injury.
  - Employee Liability Claims due to negligence or personal injury.
  - Inadequate or unsafe modifications to plant & equipment.

15. Supplier / Contract Management

- Inadequate management of external Suppliers, Contractors, IT Vendors or Consultants engaged for core operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes. This also includes:

  - Concentration issues.
  - Vendor sustainability.