Risk Management Framework

March 2024

Table of Contents

Introduction

The Risk Management Framework (the Framework) sets out the Shire of York's (the Shire) approach to the management of risk by outlining the following elements:

- Roles and Responsibilities.
- Risk Appetite Statement.
- Risk Assessment and Acceptance Criteria.

The Risk Management Framework is adopted by Council and compliments Policy G19 - Risk Assessment & Management (the Policy) which documents the commitment and objectives regarding managing uncertainty that may impact the Shire's strategies, goals or objectives.

Purpose

This Risk Management Framework assists the Shire's in understanding and documenting its 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.

By adopting the principles of the Framework, the Shire will 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 Shire along with existing time, resources and work pressures.

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 or both.

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 Objectives

- Optimise the achievement of our vision, experiences, 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 Management Governance

Governance Model

The Shire 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 the Strategic, Corporate and Operational Plans.

First Line of Defence

All **operational** areas of the Shire 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.

Second Line of Defence

The Shire’s Risk Management lead – the Executive Manager Corporate and Community Services - 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 Executive Leadership Team supplements the second line of defence.

Third Line of Defence

Internal Audits and External Audits are the **‘3rd Line’** of defence, providing assurance to the Council, Audit & Risk Committee and Shire Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit — Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the CEO.

External Audit — Received by Council on the recommendation of the Audit & Risk Committee reporting independently to the President and CEO on the annual financial statements only.

Roles, Responsibilities & Accountabilities

Council

- Review and approve Policy G19 - Risk Assessment, the Risk Appetite and Risk Assessment & Acceptance Criteria.
- Own the Strategic Risk Register.
- Receive reports from External Auditors on financial statements.
- Establish and maintain an Audit & Risk Committee in accordance with the *Local Government Act 1995*.

Audit and Risk Committee

- Support Council in providing effective corporate governance.
- Oversight of all matters that relate to the conduct of External Audits.
- Provide guidance and oversight to Council regarding Strategic Risk.
- Independent, objective and autonomous in deliberations.

CEO / Executive Leadership Team

- Undertake internal Audits as required under *Local Government (Audit) Regulations 1996*.
- Liaise with Council in relation to risk acceptance requirements.
- Monitor the appropriateness and effectiveness of the Risk Management Framework.
- Embed a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk matters.
- Own and manage the Operational Risk Register at a Shire level.

Risk Working Group

- Oversee and facilitate the Operational Risk Register.
- Champion risk management within operational areas.
- Support reporting requirements for risk matters.
- Analyse and discuss emerging risks, issues and trends.

Managers / Teams

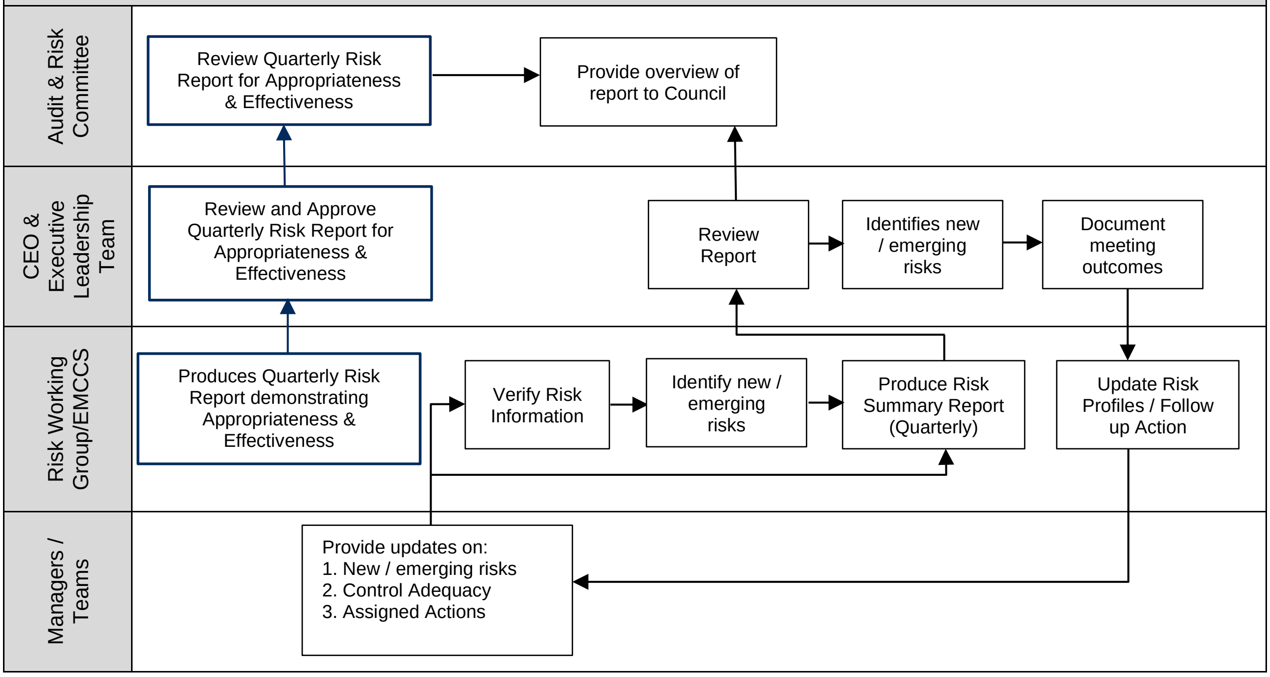
- Drive risk management culture within work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Identify emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Team Meetings.

Monitor & Review

The Shire 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.

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

Risk Management Reporting Workflow


Audit & Risk Committee
Review Quarterly Risk Report for Appropriateness & Effectiveness
Provide overview of report to Council
CEO & Executive Leadership Team
Review and Approve Quarterly Risk Report for Appropriateness & Effectiveness
Review Report
Identifies new / emerging risks
Document meeting outcomes
Risk Working Group/EMCCS
Produces Quarterly Risk Report demonstrating Appropriateness & Effectiveness
Verify Risk Information
Identify new / emerging risks
Produce Risk Summary Report (Quarterly)
Update Risk Profiles / Follow up Action
Managers / Teams
Provide updates on:
1. New / emerging risks
2. Control Adequacy
3. Assigned Actions

Risk Management Procedures

Risk Assessment and Acceptance Criteria

The Risk Assessment and Criteria are applied to the risk assessment and treatment process.

The Shire of York has identified 8 Strategic Risk Categories. These are:

- Injury or Death
- Failure/Loss of Infrastructure
- Theft Fraud Misconduct
- Climate Change/Environmental Damage
- Failure to Delivery Key Projects
- Loss of Financial Viability
- Reputational Damage
- Failure of Legislative Compliance

Risk Likelihood

The predicted likelihood of the risk event occurring over time and activity/frequency.

SHIRE OF YORK - MEASURES OF RISK LIKELIHOOD			
Rating	**Definition**	**Frequency**	**Chance of Occurring**
Almost Certain (5)	The event is expected to occur in most circumstances	More than once per year	> 90% chance of occurring
Likely (4)	The event will probably occur in most circumstances	At least once per year	60 - 90% chance of occurring
Possible (3)	The event could occur at some time	At least once in 5 years	40 - 60% chance of occurring
Unlikely (2)	The event should occur at some time	At least once in 10 years	10 - 40% chance of occurring
Rare (1)	The event may only occur in exceptional circumstances	Less than once in 15 years	< 10% chance of occurring

Risk Matrix

The overall risk level for a particular risk is assessed based on the likelihood and consequence scores for the risk plotted in the risk matrix.

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

Risk Control 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.

Risk Notification

Once the risk has been assessed, then the following table sets out the escalation requirements so that decisions can be made around accepting or treating the risk.

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 the managers / executive and subject to monthly monitoring	Executive Management Team
EXTREME (20-25)	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

Risk Treatment

Risk is treated through one of the following treatments and in accordance with the Shire's Risk Appetite. The Shire may:

Accept: Accepting or retaining the risk at its residual risk rating level, without further treatment even though it may exceed the organisation's risk appetite.

Treat: Further treating risks to reduce the likelihood and/or consequences of the risk.

Transfer/Share: Transferring part of the risk (either management of the activity/service or consequence) to another party. Sharing risk does not lesson the Shire's responsibility/accountability for that risk.

Avoid: Avoiding a risk/event with detrimental consequences by deciding not to proceed with the activity likely to create the risk, or by disposing of the risk.

Risk Appetite

Risk appetite relates to the amount and type of risk the Shire is willing to take in order to achieve its strategic objectives. When discussing risk appetite, tolerance levels will be defined as low, medium or high.

The Shire's overall risk appetite is "risk averse". The Shire is focussed on continuous improvement and delivering innovation where opportunities enhance service delivery. The Shire will consider taking calculated risks but will ensure that risks are properly identified, evaluated and managed to ensure that risk exposure is within acceptable limits. The Shire's risk appetite will be higher when it can be demonstrated that the benefits created through innovative concepts outweigh the associated risks.

Table 1: Risk Appetite Summary

Risk Appetite Range	**Low Appetite**	**Moderate Appetite**	**High Appetite**
Approach to Risk	Accept as little risk as possible and take a cautious approach	Balanced and informed approach to risk taking	A more aggressive approach for increased benefit or to achieve a key Strategic Outcome
Strategic Risk Category			
Injury or Death	Office based staff undertaking high risk activities subject to proper controls being in place	Outside staff undertaking manual labour/plant	Outside staff undertaking labour and plant activity subject to proper controls being in place
Failure/Loss of Infrastructure	Activities that result in ongoing disruption to core services	Activities that result in a disruption to a small number of services	Time limited service disruption that will enable improved service delivery to the community
Theft/Fraud/Misconduct	This is not acceptable		
Climate Change/Environmental Damage	Inadequate Environmental Management hazard risk mitigation	Activities that may result in minor environmental impacts	Activities that have environmental approvals from both state and federal agencies and will enable improved services/amenity to the wider community
Project Delivery	Activities that result in 10% or lower cost or time variations	Small, low profile changes	Innovation, ongoing community benefit shared across other partners
Loss of Financial Viability	Activities that impact financial liquidity	Activities with a low value	Activities with a low value that are likely to provide economic or revenue growth opportunities

Reputational Damage	Activities that impact a large part of the community	Activities that impact a small number of the community and are for the greater good	Activities that impact one group with overall benefits that far outweigh the inconvenience
Failure of Legislative Compliance	Minor unintentional breaches of legislation	Moderate unintentional breaches of policy or procedures	Significant unintentional breaches of process that occur in an emergency situation

Appendix A – Risk Assessment and Acceptance Criteria

SHIRE OF YORK - MEASURES OF RISK CONSEQUENCE

Rating	People	Service Interruption	Reputational (Social/Community)	Compliance	Property	Natural Environment	Financial Impact	Project - Time	Project - Cost
Insignificant (1)	Near miss/minor injuries	No material service interruption - less than 1 hour	Unsubstantiated, localised low impact on community / stakeholder 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 $5,000	Exceeds deadline by 5% of project timeline	Exceeds project budget by 10%
Minor (2)	First Aid Treatment	Short term, temporary interruption - backlog cleared < 1 day	Substantiated, localised impact on community / stakeholder trust or low media item	Some temporary non-compliances	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response	$5,001 - $25,000	Exceeds deadline by 10% of project timeline	Exceeds project budget by 15%
Moderate (3)	Medical type injuries / Lost time injury < 30 days	Medium term, temporary interruption - backlog cleared by additional resources < 1 week	Substantiated, public embarassment, moderate impact on community / stakeholder 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	$25,001 - $100,000	Exceeds deadline by 15% of project timeline	Exceeds project budget by 20%
Major (4)	Lost time injury > 30 days Temporary disability	Prolonged interruption of services - additional resources: - performance affected < 1month	Substantiated, public embarassment, widespread, high impact on community / stakeholder trust or high media profile, 3rd party actions	Non-compliance results in termination of services or imposed penalties to Shire/Officers	Significant damage requiring internal and external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies	$100,001 - $500,000	Exceeds deadline by 20% of project timeline	Exceeds project budget by 25%
Extreme (5)	Fatality / permanent disability	Indeterminate prolonged interruption of servicves - non-performance > 1 month	Substantiated, public embarassment, widespread loss of community / stakeholder trust or high, widespread multiple media profile, 3rd party actions	Non-compliance results in litigation, criminal charges or significant damage or penalties	Extensive damage requiring long period of restitution. Complete loss of plant, equipment & building.	Uncontained, irreversible impact	More than $500,000	Exceeds deadline by 25% of project timeline	Exceeds project budget by 30%

Appendix B – Strategic Risk Definitions

1. Injury or Death

A failure to take reasonable care in any Shire process, project or actions which results in the injury or death of any person.

2. Failure/Loss of Infrastructure

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.

3. Theft/Fraud/Misconduct

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).

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.

4. Climate Change/Environmental Damage

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

The scope includes:

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

5. Failure to Deliver Key Projects

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.
- Insufficient oversight.

6. Loss of Financial Viability

Failure to adequately plan for the long term future of the Shire.

Failure to ensure adequate oversight of financial systems, policies and processes by Elected Members and Shire employees which result in a loss of service.

7. Reputational Damage

Failure to adequately consult with or communicate to members of the community or other stakeholders resulting in negative opinion.

Failure to prevent any action, policy or process of the Shire resulting in a reduction in trust and a drop in the positive public perception of the Shire.

8. Failure of Legislative Compliance

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 Act (refer "Injury or Death").

It does include the Local Government Act, Health Act, Building Act, Privacy Act and all other legislative based obligations for Local Government.