Risk Management Strategy

2019

TABLE OF CONTENTS

Risk Management Strategy 3
1.1 Introduction 3
1.2 Risk Management – Principles, Framework and Process 4
1.3 Risk Management Policy 5
1.4 Risk Management Principles 5
1.5 Risk Management Framework 6
1.6 Risk Management Process 7
1.7 Risk Management Process – Communication and Consultation 8
1.8 Risk Management Process – Risk Categories / Risk Themes 9
1.9 Risk Management Process – Risk Tolerance / Risk Appetite 10
Table 1: Roles and Responsibilities 12
Table 2: Consequence Ratings 13
Table 3: Risk Matrix 14
Table 4: Likelihood Rating 14
Table 5: Risk Response 14
Terminology 16

RISK MANAGEMENT STRATEGY

1.1 Introduction

The Risk Management Strategy (Strategy) aims to support an **integrated** and effective approach to risk management to ensure an organisation-wide approach to risk management, with the aim of value creation and protection, in accordance with the Shire of Northampton Risk Management Policy. This includes consistent assessment of risks including risk mitigation activities from a top down perspective, as well as bottom up, through operational processes and procedures.

The Shire has implemented a structured approach to risk management based on, Australian / New Zealand International Standard for Risk Management – Guidelines ISO 31000:2018. This will assist the Shire work towards:

- Aligning the objectives, culture and strategy of the Shire with risk management;
- Addressing and recognising all obligations (including voluntary commitments) of the Shire;
- Communicating the risk appetite of the Shire to guide the establishment of risk criteria, whilst conveying to all elected members, employees and contractors;
- Promoting and conveying value of risk management across the Shire;
- Encouraging methodical monitoring of risks; and
- Ensuring the Risk Management Strategy remains relevant to and considers the context of the organisation.

The key **objectives** of the Strategy are to:

- Ensure consistent and systematic approach to risk management through decision-making and corporate planning, contributing toward an effective and efficient risk management culture over time;
- Provide tools to assist management with risk identification and articulation of risks to enable appropriate risk mitigation strategies; and
- Supports the overall governance framework through integration of corporate culture, internal controls, policies and procedures (“internal control environment”) and management oversight.

The Strategy has been developed with input and review from Senior Staff and the Audit Committee.

RISK MANAGEMENT STRATEGY

1.2 Risk Management – Principles, Framework and Process

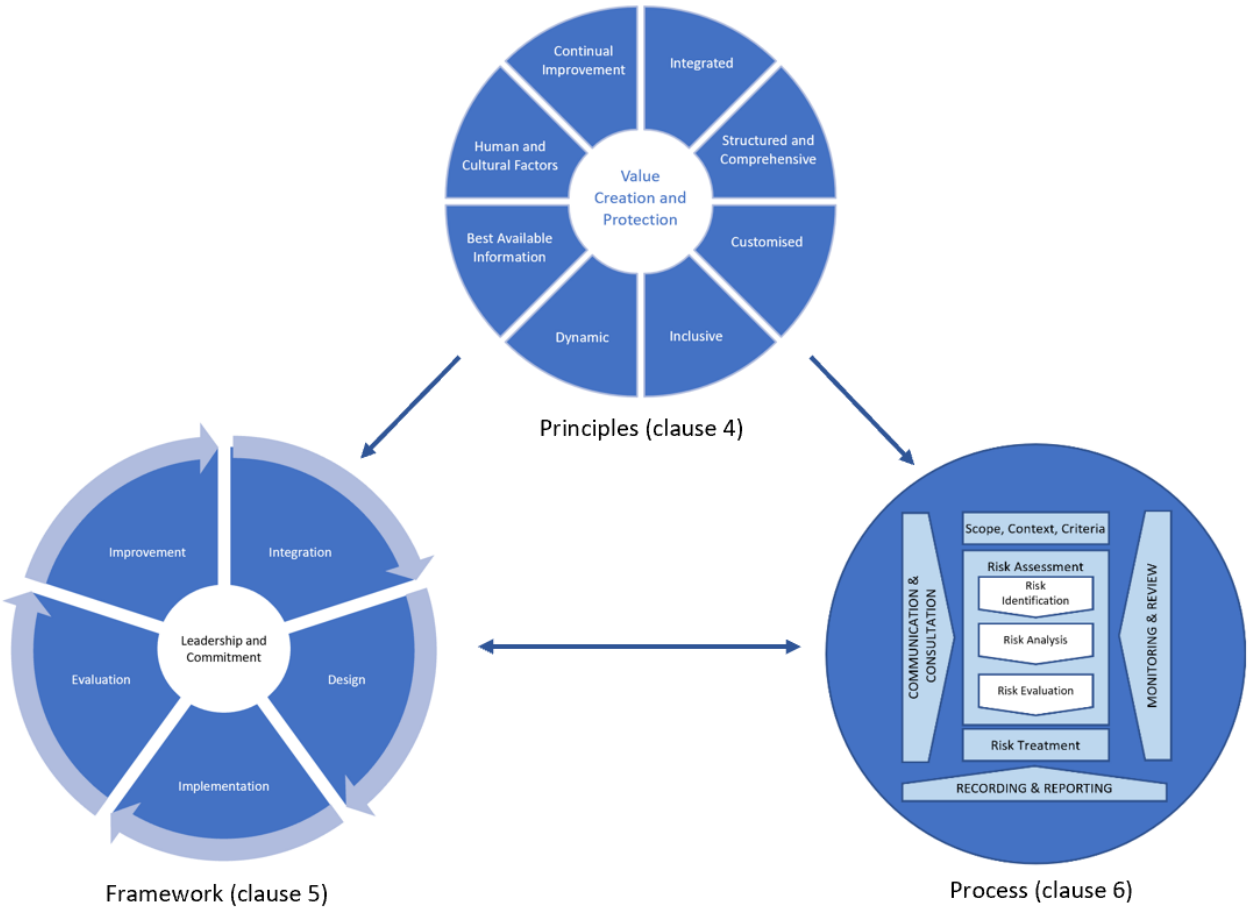
ISO 31000:2018 provides guidance on the development of a risk management approach, designed to be tailored to best apply to any organisation and its requirements. This Strategy has been developed using the Principles, Framework and Process as outlined within ISO 31000:2018.

The diagram below demonstrates the relationship between each component of the Risk Management Strategy, with the Principles forming the foundation of the Strategy. The Principles describe the features to be utilised and influence the Framework and Process elements.

The Framework component of the Strategy is intended to facilitate integration of risk management throughout the Shire, through commitment from leadership to risk management practices. Any gaps identified through analysis of existing practices will be remedied through the application of the Framework and will inform the Process component.

The Risk Management Process is to be designed and tailored to align best to the Shire's structure, resources and practices. The Risk Process is iterative, consisting of Risk Assessment, Risk Identification, Risk Analysis, Risk Evaluation and Risk Treatment, Communication and Consultation, Recording and Reporting along with Monitoring and Review, as noted in the below diagram. The Process component of the Strategy draws on both the Framework and the Principles in its application to managing risk.

High Level Overview of Strategy



Source: Australia/New Zealand Standard ISO 31000:2018

RISK MANAGEMENT STRATEGY

1.3 Risk Management Policy

The Shire's Risk Management Policy (A.2.13) states the mandate and commitment including roles and responsibilities of Council and all staff:

"*Management of risk is considered the responsibility of all elected members, employees and contractors, and is to be integrated throughout the Shire.*"

The Risk Management Policy must be read and understood in conjunction with this Strategy.

1.4 Risk Management Principles

In accordance with ISO 31000:2018, the following key principles provide necessary guidance and methodology when implementing a structured risk management process.

Human and cultural factors: Risk culture is created from visible leadership and commitment in embedding a risk mindset. All elected members and employees have responsibility for managing risk.

Risk management should be a part of, and not separate from, the Shire's purpose, governance, leadership and commitment, strategy, objectives and operations.[1]

Structured and comprehensive: Refers to the risk management process which encompasses:

- Risk identification, assessment and treatment;
- Risk monitoring and review; and
- Risk reporting and communication.

Inclusive accountability and transparency: Leadership to assign clear roles and responsibilities for staff, external stakeholders and decision makers to ensure risk management remains relevant and up-to-date, and is based on informed choices and agreed priorities.

Integrated: Managing risks should create and protect value by contributing to the achievement of objectives as included in the Strategic Community Plan and Corporate Business Plan (Plan for the Future), as well as project outcomes and improving Shire performance as an integrated activity within existing processes.

Customised to Shire risk profile: Recognises the Shire's external and internal influences and challenges, due to its geographical location and community needs.

Dynamic: Risks needs to be managed in a dynamic, iterative and responsive manner.

Continuous improvement: Developing a more risk aware workforce will result in operational processes which take into account risk considerations and enable processes and decision making to improve over time.

Best available information: Risk management is reliant on use of the best available information at any given point in time.

[1] ISO 31000:2018 Risk Management – Guidelines, page 5

RISK MANAGEMENT STRATEGY

1.5 Risk Management Framework

The impact of risk management efforts is highly dependent upon the integration of risk management throughout the Shire. The Risk Management Framework is designed to assist with facilitating high level of integration across activities, practices and functions of the Shire.

Details of each stage within the framework are:

Integration

- Integrate risk management into Shire processes and structure. All elected members and employees are responsible for managing risk.

Design the Strategy

- Understand the organisation and its context;
- Establish and adopt Risk Management Policy;
- Establish roles, responsibilities and accountabilities;
- Allocate resources; and
- Establish internal and external communication and reporting mechanisms.

Implement the Strategy

- Develop Risk Management Plan;
- Engage stakeholders to convey the purpose and importance of the Strategy and Plan;
- Implement corporate risk management processes in all activities throughout the Shire, particularly decision making processes; and
- Identify changes in the internal and external context, as well as identifying emerging risks or changed risk conditions.

Evaluate the Strategy

- Regularly assess the purpose, objectives, and outcomes of the Strategy against actual risk management practices; and
- Consider the suitability and application of the Strategy to the Shire's operations and activities.

Continuous Improvement

- As gaps or improvement opportunities are identified from risk processes, continuously refine the Framework and the way the process is integrated; and
- Develop plans and tasks and assign them to those accountable for implementation.

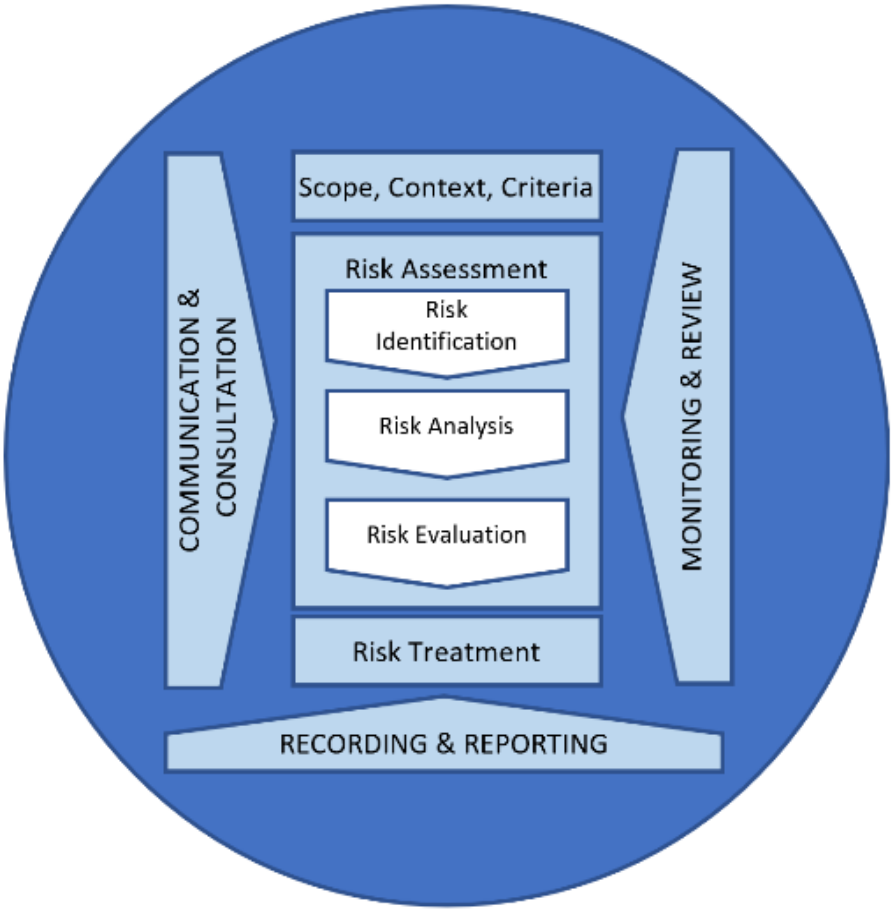
RISK MANAGEMENT STRATEGY

1.6 Risk Management Process

The risk management process can be delivered in many different ways. It should play a pivotal role in management of the Shire and decision making, unified with the general operations, practices, procedures and the structure of the Shire. Applications of the risk management process should be tailored to best work with the structure and context of the Shire and draw on the risk principles as defined in Section 1.4, with appropriate consideration afforded to maintaining the dynamic nature of the process, continual improvement, the variable nature of human and cultural factors, modifying and integration of processes/practices.

Given the highly dynamic and variable nature of the risk management process, the general approach by the Shire is to articulate and develop details relating to risk management processes within operational procedures, to best communicate the applicable elements of the process throughout the organisation. Development of these procedures will also enable appropriate feedback to be sought from stakeholders and implemented into decision making processes.

The diagram below depicts the re-iterative and continuous process for managing risks.



Source: Australia/New Zealand ISO31000:2018

RISK MANAGEMENT STRATEGY

1.7 Risk Management Process – Communication and Consultation

Communication and consultation are important elements of the risk management process. These elements promote a better understanding of risk across the Shire and convey the purpose behind actions occurring or required.

An effective risk management process relies on regular communication and consultation, both upward to leadership and downward from leadership and senior staff, involving risk owners, Shire management, Audit Committee and Council.

The main objectives of risk communication and consultation are to:

- Provide information for decision making (relevance of information is dependent on currency);
- Utilise expertise from across the organisation in the course of carrying out risk management activities; and
- Facilitate an inclusive and empowered culture across the Shire in relation to risk management.

Communication of newly identified, untreated high level risks will be as follows:

Risk Context	**Purpose**	**Reporting to:**
Strategic	Emerging risks or existing risks which impact on the Council's ability to deliver on its strategic objectives.	CEO/Council
Operating	Risks identified from operational activities which need to be addressed, reported and monitored until effectively treated to an acceptable risk tolerance.	CEO
Projects	Risks identified from capital or infrastructure projects which impact on the project deliverables above the Council's acceptable risk tolerance.	CEO
Consolidated Risk Summary	For Executive Management – summary of high level risks and above items to inform Audit Committee & Council of risk treatments.	Audit Committee / Council

In line with the multi-directional approach to risk consultation it is equally important for newly identified untreated risk to be communicated from Council to the Executive.

Each level of management must communicate risks as they become aware of them, to relevant staff at the level directly above and below them, who must in turn communicate the risks to the next level above or below.

Communication and consultation of medium and higher risks should be through a documented process. Lower level risks may be communicated verbally.

RISK MANAGEMENT STRATEGY

1.8 Risk Management Process – Risk Categories / Risk Themes

The purpose of risk categories and/or risk themes is to group similar risks under the appropriate risk category. The use of standard risk categories enables:

- Structured process for staff to identify and capture risks; and
- Reporting of risks by risk type, providing focus areas requiring risk mitigation, especially where similar risks are identified across functional areas and/or by different stakeholders.

The Shire's risk categories/themes should be continually reviewed to ensure relevance in current environment.

Examples of risk categories within the local government sector include:

1. Performance: ability to achieve key objectives, within current resources, potential loss of infrastructure;
2. Financial: loss of assets, impact on annual revenues or costs, external audit issues, mismanagement of funds;
3. Environmental Risk: harm to the environment;
4. Reputational Damage: adverse publicity;
5. Service Delivery/Business Interruption: loss of service, disruption in business processes or impact to service delivery (including through lack of skilled resources); and
6. Legislative / Regulatory / Policy / Occupational Safety and Health: misconduct, injury, failure to meet statutory, regulatory or compliance requirements.

Risk categories will be defined in the initial establishment of risk registers and should be dynamic to reflect the current environment.

RISK MANAGEMENT STRATEGY

1.9 Risk Management Process – Risk Tolerance / Risk Appetite

Risk tolerance or risk appetite can be defined as the amount and type of risk the Shire is willing to take in order to meet its strategic objectives. Given the characteristic risk profile of local governments, it is important the Elected Members and CEO understand and consider this relatively low appetite for risk when evaluating major decisions. To facilitate meaningful analysis of the Shire's risk exposures, one role of the Council is to constructively challenge management's proposals from a risk perspective.

As risk management processes mature, a risk appetite matrix which pre-defines types of risk and quantifies them in a structured manner will help ensure the Shire's strategic objectives are effectively planned and managed. It enables articulation of specific actions/practices, i.e. the Shire does not tolerate any risk of breaches to regulatory obligations or legislative requirements. This assists staff understanding of how their day to day risk management activities contribute towards the Shire's risk culture and risk profile.

Understanding risk appetite helps determine the level of acceptable/unacceptable risk and the extent to which additional controls are required to treat risk. As a public body, there is an expectation the Shire will maintain an inherent low appetite for risk and as a consequence adopt policies and procedures in order to maintain the organisation's reputation and to protect public funds from loss or misappropriation.

The appetite for risk in relation to service delivery, finance, health, safety and the environment is considered 'low to medium', requiring treatment with effective controls. Where the level of risk is considered 'high' or 'extreme', additional controls are required to reduce the risk level. In circumstances where the level of risk cannot be reduced below 'high', close monitoring of risk controls is required to ensure the relevant internal controls remain effective. In cases of medium to high risk, the Shire will mitigate the risk by taking out insurance where possible.

RISK MANAGEMENT STRATEGY

Documentation to support risk management process

Documentation of medium and high level risks is best undertaken through the use of a risk register. Maintenance of risk registers demonstrates an active and evidentiary risk management process within the Shire.

The following provides guidance for documentation of risk registers:

- All elected members and employees have responsibilities to identify, assess, evaluate and treat risks in their day to day activities; risks assessed as being mitigated to an acceptable level through operating controls or risk treatments by eliminating the risk are deemed to be effectively addressed and do not require documenting;
- Risks which require further actions or treatment by more senior officers before they are within the acceptable risk tolerance must be documented in the risk register to enable effective communication and monitoring; and
- Any risks deemed to be rated High or Extreme and unable to be immediately treated to an acceptable level, must be escalated to the CEO immediately for further escalation to the Audit Committee and/or Council, where unable to be adequately treated by the CEO within the constraints of the annual budget. These risks must also be recorded in the risk register.

Assurance activities for risks mitigated through operational and/or financial controls

The Shire has the following governance activities to ensure controls required for risk mitigation are operating as intended:

- Completion of mandatory returns as required by legislation;
- Routine independent verification of operating controls, systems and procedures;
- External audit of financial statements; and
- Via Code of Conduct, Council policies and work procedures.

The following pages contain tools and guidance useful in the implementation of this Strategy.

- Table 1: Roles & Responsibilities
- Table 2: Risk Ratings
- Table 3: Matrix Assessment
- Table 4: Likelihood Rating
- Table 5: Risk Response

RISK MANAGEMENT STRATEGY

Table 1: Roles and Responsibilities

Role	Responsibilities
Council	Council's responsibilities are to: • Adopt a Risk Management Policy compliant with the requirements of AS/NZS ISO 31000:2018 and to review and approve the Policy in a timely manner as required. • Be satisfied risks are identified, managed and controlled appropriately, to achieve Shire's strategic objectives. • Supports the allocation of funds / resources to treat risks as required.
Audit Committee	• Requests and reviews reports on risk management on a biannual basis (minimum) or as required depending on the nature of the risk(s). • Monitors the overall risk exposure of the Shire and makes recommendations to Council as appropriate. • Assesses for effectiveness the risk control measures / risk treatment plans in reducing the severity of the risk(s).
Executive	• Creates an environment where staff are responsible for and actively involved in managing risk. • Oversight of the Shire's Risk Management Strategy. • Maintain and implement the Risk Management Strategy. • Ensures a consistent risk management approach is embedded in the operations and processes of the Shire. • Actively participates and supports the Risk Management Strategy through identification and creation of suitable risk treatments to control strategic and operational risks facing the Shire. • Monitors the strategic and operational risk management performance. • Reviews the Shire's Risk Summary Report prior to submission to the Audit & Risk Committee.
Staff	• Adopt and understand the principles of risk management and comply with policies, processes and practices relating to risk management. • Alert and bring to management's attention, the risks existing within their area. • Conduct risk assessments which are appropriate with the scope of the task and the associated level of risk identified.

RISK MANAGEMENT STRATEGY

Table 2: Consequence Ratings

Description	Performance	Financial	Environment	Reputation	Service Delivery / Business Disruption	Legislative / Regulatory / Policy /OSH
CATASTROPHIC	Unable to achieve key objectives. External resources required. Ongoing loss of critical infrastructure.	>15% of asset value. Adverse >15% deviation from budget. Audit unable to be completed.	Catastrophic long term environmental harm.	Significant damage to public confidence leading to sustained compromise in the achievement of strategic objectives.	Major, including several important areas of service and/or a protracted period. Ongoing loss of business systems.	Criminal instances of regulatory non-compliance. Extreme breaches of Code of Conduct. Personal details compromised / revealed – all. Death.
MAJOR	Major impact on ability to achieve key objectives. Impact cannot be managed with current allocated resources. Long-term loss of critical infrastructure.	5%-15% of asset value. Adverse 5%→15% deviation from budget. Audit qualification on the report and accounts.	Significant long-term environmental harm.	Local publicity of a major and persistent nature, affecting the perception/ standing within the community.	Complete loss of an important service area for a short period. Major disruption to business processes.	Major revenue or cost implications. Individuals at risk of harm. Significant breaches of Code of Conduct. Personal details compromised / revealed – many. Multiple serious injuries.
MODERATE	Moderate impact on ability to achieve key objectives. Significant adjustment to resource allocation. Loss of support infrastructure.	2%-5% of asset value. Adverse 2%→5% deviation from budget. Management letter contains significant issues.	Significant short-term environmental harm.	Damage to reputation to a specific audience, may not have significant long-term or community effects.	Major effect to an important service area for a short period, brief impact on multiple areas. Moderate disruption to business processes.	Minor revenue or cost implications. Breach of Code of Conduct. Personal details compromised / revealed – some. Serious injury and/or illness.
MINOR	Minor impact on ability to achieve key objectives. Additional internal management efforts required. Interruption to support infrastructure.	< 2 of asset value. Adverse impact on revenues and costs <2% deviation from budget. Management letter contains minor issues.	Minor transient environmental harm.	Minor damage to reputation to a small audience, complaint from a large group of people.	Brief disruption of important service area. Noticeable effect to non-crucial service area. Minor disruption to business processes.	Minor breaches of Code of Conduct. Personal details compromised / revealed – isolated. First aid or minor lost time injury.
INSIGNIFICANT	Negligible impact on ability to achieve key objectives. Impact can be managed through routine activities. Negligible interruption to support infrastructure.	Insignificant loss. Insignificant adverse impact on annual revenue or costs. Matters discussed with management not reported.	Negligible transient environmental harm.	Minor unsubstantiated publicity or damage to reputation to a small audience, complaint from individual/small group.	Negligible impact on the effectiveness of the organisation's processes. Negligible disruption to business processes.	Little or no impact to Code of Conduct. Personal details compromised / revealed - an individual's. Incident with or without minor injury.

RISK MANAGEMENT STRATEGY

Table 3: Risk Matrix

		CONSEQUENCE				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
		1	**2**	**3**	**4**	**5**
Almost Certain	5	Medium	High	High	Extreme/Exceptional	Extreme/Exceptional
Likely	4	Medium	Medium	High	High	Extreme/Exceptional
Possible	3	Low	Medium	Medium	High	High
Unlikely	2	Low	Low	Medium	Medium	High
Rare	1	Very low	Low	Low	Medium	Medium

Table 4: Likelihood Rating

Likelihood	Definition	Frequency of Noted Occurrences	Score
Almost Certain	Expected to occur in most circumstances or occurs regularly. A clear opportunity already apparent, which can easily be achieved.	More than once per year	5
Likely	Occurrence is noticeable or is likely to occur. An opportunity that has been explored and may be achievable.	At least once per year	4
Possible	Occurs occasionally or may occur. Possible opportunity identified.	At least once in 5 years	3
Unlikely	Occurs infrequently or is not likely to occur. Opportunity that is fairly unlikely to happen.	At least once in 10 years	2
Rare	Only occurs in exceptional circumstances. Opportunity that is very unlikely to happen.	Less than once in 20 years	1

Table 5: Risk Response

Risk	Action Required
Extreme/Exceptional	Immediate corrective action
High	Prioritised action required
Medium	Planned action required
Low	Planned action required
Very low	Manage by routine procedures

RISK MANAGEMENT STRATEGY

Date approved:	18/12/19
Responsible officer:	CEO
Endorsed by:	Audit Committee
Approved by:	Council
Next review:	2021

TERMINOLOGY

Definitions	
Consequence	The outcome of an event affecting achievement of organisational objectives.
Control	A measure that modifies a risk or manages risks within an organisation.
Establishing the context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and evaluating the significance of a risk (i.e. risk criteria).
Event	The occurrence or change of a particular set of circumstances.
Likelihood	The chance of a risk event occurring.
Monitoring	Continual checking, critically observing or determining status in order to identify change from the performance level required or expected.
Operational risk	Operational risks are linked to the Business Plan objectives and take into consideration risks which will prevent departments from delivering their annual business plans and ongoing services to the community.
Residual risk	The risk remaining after risk treatment.
Risk	The effect of uncertainty on objectives. The focus should be on the effect of incomplete knowledge of events or circumstances on the Shire's decision making.
Risk analysis	The process to comprehend the nature of risk and to determine the level of risk.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk attitude	The organisation's approach to assessing and eventually pursuing, retaining, taking or turning away from risk.
Risk criteria	The terms of reference against which the significance of a risk is evaluated.
Risk evaluation	The process of comparing the results of a risk analysis with the risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk identification	The process of finding, recognising and describing risks.
Risk management	The co-ordinated activities to direct and control an organisation with requirements to manage risk.

TERMINOLOGY

Definitions	
Risk management policy	The Shire's statement of overall intention and direction related to risk management.
Risk owner	The person with the accountability and authority to manage a risk.
Risk profile	The acceptable level of risk an organisation is prepared to accept. For the purposes of this Framework, the Shire's risk profile is the overall exposure to risk based on its aggregated risks, at a point in time.
Risk source	An element that, either alone or in combination, has the intrinsic potential to give rise to a risk.
Risk treatment	The process to modify risk.
Stakeholder	A person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.
Strategic risk	Strategic risks are the risks that will prevent the Shire from meeting the objectives outlined in its Plan for the Future.
Reference: ISO 31000:2018 Risk management—Guidelines	