# Risk Management Policy
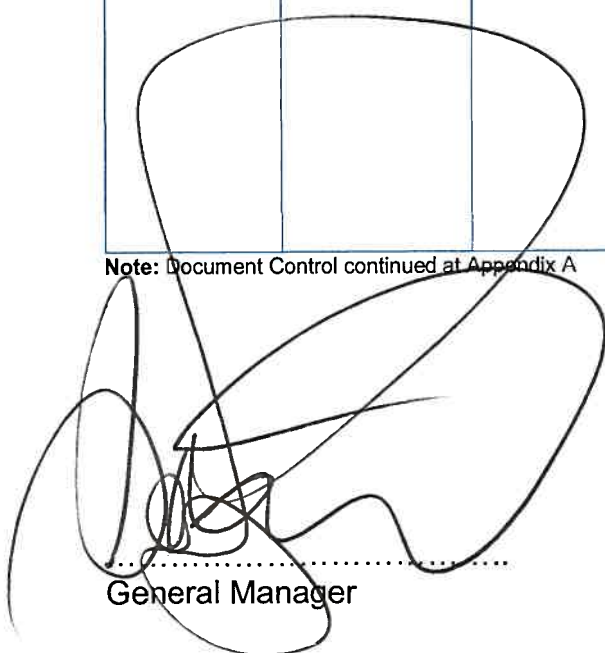
# 1 DOCUMENT AUTHORISATION

| RESPONSIBLE OFFICER: | MANAGER OF GOVERNANCE, RISK AND CORPORATE PLANNING (MGRCP) | | | | |
|---|---|---|---|---|---|
| **REVIEWED BY:** | MGRCP, MANEX. | | | | |
| **REVIEW DUE DATE:** | March 2024 | | | | |
| **VERSION NUMBER:** | 5 | | | | |
| **DOCUMENT NUMBER:** | NA | | | | |
| **VERSIONS:** | **DATE:** | **RESOLUTION NO:** | **DESCRIPTION OF AMENDMENTS:** | **AUTHOR / EDITOR:** | **APPROVED / ADOPTED BY:** |
| 5 | 25/03/2021 | 8.04/21 | Amendments are substantial consisting of a complete overhaul of the entire Policy to reflect the entire risk management framework, Council's approach to risk management and roles and responsibilities. | MGRCP | Council |
| 4 | 28/09/2017 | 16.09/17 | Minor amendments included:<br><br>• Updating the reference to the new Community Strategic Plan 2017-2027;<br><br>• Minor changes to the diagram within the Policy;<br><br>• Extension of the review period of the Policy from two (2) years to three (3) years in line with other similar policies. | MRC | Council |

Note: Document Control continued at Appendix A

.................................................
General Manager

$3/5/21.$
.................................................
Date

# 2 CONTENTS

# 3 DEFINITIONS

| | |
|---|---|
| *Consequence:* | An outcome of an event affecting objectives. |
| *Control:* | A measure that maintains and/or modifies *risk*. |
| *Control Owner:* | A control owner is the officer of council assigned responsibility for the management of a control within Council's electronic risk management system and register – Pulse ERM. The control owner may push tasks for the implementation of the control. |
| *Event:* | An occurrence or change of a particular set of circumstances. |
| *Likelihood:* | The chance of something happening. |
| *Pulse ERM:* | Council's Digital enterprise risk management software system for entering significant risks, details of the risk, causes, consequences, mitigation strategies, risk assessment (both inherent and residual), developing controls, assigning controls and actions, linking to Council's Integrated Planning and Reporting framework, monitoring and reviewing risk. This is a sophisticated risk management register. |
| *Risk:* | Effect of uncertainty on objectives. |
| *Risk Appetite:* | Provides a guide to management and risk owners in respect to the parameters of acceptable risk taking and tolerances. |
| *Risk Management:* | The coordinated activities to direct and control an organisation regarding risk. |
| *Risk Management Framework:* | The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. |
| *Risk Management Process:* | Systematic application of risk management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| *Risk Owner:* | A risk owner is the officer of council assigned responsibility for the management of a risk within Council's electronic risk management system and register – Pulse ERM. The risk owner may create risks, controls and push tasks. |
| *Stakeholder:* | A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity. |

# 4 PURPOSE

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The purpose of this policy is to:

- Ensure that risk management is a fundamental component of decision making in all Council activities, and all decisions made by Council and its Officers will consider the risks involved in taking those decisions and the impact of those decisions on the achievement of Council's objectives;

- Ensure that the implementation of the risk management framework will enhance the delivery of the community vision and strategic goals as outlined in the **Glen Innes Severn Community Strategic Plan (CSP)**;

- Ensure Council's risks are managed in a manner consistent with Council's risk appetite;

- Ensure Council's risks are managed using sound risk management practices;

- Ensure decisions are made with an understanding of Council's risk environment;

- Facilitate taking risks and capitalising on opportunities, within Council's risk appetite, to assist Council to meet its strategic objectives;

- Promote a culture of risk awareness throughout the organisation;

- Highlight the core components of Council's enterprise risk management framework; and

- Define the key responsibilities of Council Officials.

# 5 APPLICABILITY

This policy applies to:

- Councillors;
- All Council Staff;
- Volunteers and delegates of Council;
- Contractors;
- Members of Section 355 Committees of Council; and
- Members of Council's Advisory Committees.

# 6 OUTCOMES

Council maintains a durable commitment to entrenching effective risk management into all activities and as such, risk management is a core responsibility of management.

Management has the responsibility to evaluate the risk environment, to put in place appropriate controls and to monitor the effectiveness of these controls, as well as communicate the risk management framework, plan and procedures throughout Council. This process is supplemented with a review of key corporate risks by the **Management Executive Team (MANEX)**.

The outcomes of this policy are to facilitate Council striking a balance between risk management and opportunity taking, whilst achieving the objectives set out in Council's CSP by:

- Ensuring enterprise risk management is integrated into Council's strategic and operational planning processes to:
  - Avoid, eliminate or minimise harm and/or loss; and
  - Minimise the adverse impacts that uncertainty presents to the achievement of Council's CSP.
- Supporting and enabling effective:
  - Delivery of equitable and appropriate services and facilities for the community;
  - Innovation and business improvement; and
  - Risk management practices that lead to a risk aware culture.
- Having regard to long-term and cumulative commitments by Council to environment, economic, social and governance objectives aligned with its **Integrated Planning and Reporting Framework (IPRF)**.

# 7 POLICY STATEMENT

## 7.1 Principles

Effective risk management requires the following key elements:

- Risk management is to be an integral part of all Council's activities;
- A structured and comprehensive approach to risk management contributing to consistent and comparable results;
- The risk management framework and process are customised and proportionate to Council's external and internal context related to its strategic objectives;
- Is inclusive and provides appropriate and timely involvement of stakeholders, enabling their knowledge, views and perceptions to be considered, resulting in improved awareness and informed risk management;
- Is dynamic to allow for the changes in both internal and external context as risks can emerge, change or disappear. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner;
- Is based on the best available information. The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders;
- Considers human and cultural factors. Human behaviours and culture significantly influence all aspects of risk management at each level and stage; and
- Is continually improved through learning and experience.

## 7.2 Risk Management Framework

Council's risk management approach consists of the following key elements:
- Risk Management Policy;
- Risk Appetite Statement;
- Risk Management Plan and Procedures; and
- Pulse ERM.

## 7.3 Risk Management Culture

Risk management culture refers to the set of shared values and behaviours that characterise how Council considers risk in its day-to-day activities. Risk management culture should be embedded into and not separate from the organisational culture. Risk culture is the glue that binds all the elements of risk management together because it reflects the shared values, goals, practices and mechanisms that integrate risk into Council's decision-making processes and risk management into its operating processes.

Council fosters a positive risk management culture where risk management is seen as a positive attribute of decision-making rather than a corrective measure. Staff are encouraged to have a willingness to engage effectively with risk.

## 7.4    Risk Profile and Appetite

Council seeks to manage its risk profile carefully. This reflects the view that satisfactory fulfilment of its important public responsibilities could be seriously jeopardised if poorly managed risks were to lead to significant impairment of operations, financial losses, harm to the environment and/or damage to Council's reputation.

In support of this, Council will develop a risk appetite for Council's most significant risks. This will define the amount of risk Council is willing to accept in pursuit of its strategic goals and will form the basis of Council's approach to managing risk and taking opportunities in day to day operational activities as well as strategic decision making.

The Risk Appetite Statement with have flexibility to consider the factors in which (more or less) risk will be considered in pursuit of the organisation's objectives.

## 7.5    Risk Management Plan

A risk management plan will be developed to provide structure for how Council will implement the Risk Management Policy and conduct its risk management activities. The primary purpose of the plan is to ensure that the Council's arrangements for managing risks are clearly understood and practiced, and identifies where, when and how different types of decisions relating to risk are made across the Council and by whom.

The Risk Management Plan will include:
- Roles, accountabilities and responsibilities in relation to risk management;
- The timeframes for risk management activities;
- The activities that Council will undertake to implement its risk management policy;
- How risk management processes will be implemented and maintained;
- Resourcing requirements (people, IT and physical assets);
- Training and development requirements;
- Performance measures that will be used to evaluate the success of the Council's risk management framework;
- Guidance, resources and objective parameters to assessing risk and using Pulse ERM effectively; and
- How and when the Council's Risk Management Framework will be reviewed.

## 7.6    Risk Management Procedures

Risk management procedures shall be developed or adopted as necessary, to provide a systematic way of identifying, assessing and prioritising risks, deciding how they will be managed, and documenting and communicating this across the Council.

All risk management procedures are to be performed in accordance with AS ISO 31000:2018, using qualitative, semi-quantitative or quantitative methods and techniques that best suit the Council's operations, risk management maturity and decision-making needs.

## 7.7 Decision Making

To ensure its success, the Risk Management Framework will be integrated within all the Council's decision-making processes, governance structures, operational procedures and integrated planning and reporting processes.

## 7.8 Risk Management Framework – Continuous Review

MANEX is responsible for ensuring the effectiveness of the risk management framework can be assessed. This will be achieved by ensuring that:
- Any Mitigation Strategies developed have performance targets and timelines that can be measured against goals and objectives; and
- a *methodology* is implemented to obtain the data from Pulse ERM needed to measure the impact of Council's risk management framework.

The ongoing monitoring and review of the information gathered from Council's risk management processes will be undertaken by MANEX to ensure the risk management framework is up-to-date and relevant.

# 8 ROLES AND RESPONSIBILITIES

## 8.1 Council

Council are responsible for overseeing risk management and ensuring that:
- Strategic risks are adequately considered when setting the organisations objectives;
- Risks facing the organisation in pursuit of its objectives are clearly understood;
- Risk management systems are implemented and operating effectively;
- Information about risks and risk management of the organisation are communicated properly;
- Council's Risk Appetite is determined;
- Oversight of Council's enterprise risk management framework is provided;
- Risks are considered in all decision making to ensure alignment with Council's risk appetite statements; and
- As a part of the approval of the annual budget, ensure the provision of resources are available to achieve the outcomes of this Policy.

## 8.2   General Manager

Consistent with the General Manager's role under section 335 of the *Local Government Act 1993* (the Act) to conduct the day-to-day management of Council, the General Manager has ultimate responsibility and accountability for risk management in Council. This includes:
- Ensuring Council operates within its risk appetite;
- Overseeing Council's risk management framework and ensuring that it is effectively communicated, implemented and reviewed regularly;
- Promoting a positive risk culture;
- Ensuring that all Council managers and staff understand their risk management responsibilities and that these are included in all job descriptions, staff induction programs, performance agreements and appraisals; and
- Attesting in the Annual Report that Council's risk management framework complies with statutory requirements and remains relevant and in line with best practice.

## 8.3   Management Executive Team (MANEX)

The Directors and the General Manager form MANEX. As a team they are responsible for:
- Approving Council's risk management plan, risk register (Pulse ERM), and risk profile;
- Managing high level strategic risks facing Council;
- Promoting and championing a positive risk culture; and
- Approving Council's implementation of corrective actions, as recommended by Council's internal audit function, external audit and the **Audit, Risk and Improvement Committee (ARIC)**.

## 8.4   Risk Owners

Directors, managers and other assigned risk owners have the responsibility for managing specific policy, project and program risks across Council. Within their range of authority, this includes being responsible for:
- Promoting awareness of risks and controls that must be implemented;
- Ensuring Council staff are implementing Council's risk management framework and performing their risk management responsibilities;
- Identifying risks that will affect the achievement of Council objectives;
- Establishing and/or implementing specific policies, operating and performance standards, budgets, plans, systems and/or procedures to manage risks;
- Monitoring the effectiveness of risk treatment and internal controls; and
- Documenting all the above in Pulse ERM.

## 8.5    Manager of Governance, Risk and Corporate Planning (MGRCP)

The MGRCP is the responsible officer for this Policy and will coordinate the following functions in relation to the Policy:

- Maintaining appropriate records relating to the Risk Management Framework;
- Implementing effective risk management communication mechanisms within Council;
- Developing and maintaining a risk reporting framework to enable regular advising/reporting of key risks and the management of those risks to MANEX and the ARIC;
- Supporting MANEX by co-ordinating and providing clear and concise risk information, advice and/or reports that can be used in planning and decision making;
- Provide training, support, advice and guidance to managers and relevant Council staff to assist them in managing risk and implementing the framework within their area/s or responsibility;
- Undertaking regular reviews of the Framework, Policy, Plan and any associated procedures;
- Helping to build a risk management culture within Council;
- Coordinating the various activities relating to risk management within Council;
- Ensuring that there are easily accessible systems and processes in place to enable all staff to conveniently undertake risk management in their daily functions;
- Establishing and/or maintaining an ongoing monitoring system to track risk management activities undertaken within Council and assessing the need for further action; and
- Assessing risk management information for completeness, accuracy and consistency.

The Risk Management Plan will outline any responsibilities/functions, as listed above, that are allocated, in part or in full, to other Risk or Control Owners within Council, as appropriately required.

## 8.6    Staff

All Council staff are responsible for considering risk and risk management in all their day-to-day functions, such as:

- Helping to identify risks in their business unit;
- Implementing risk controls within their area of responsibility;
- Following best practice and standard operating procedures (where applicable); and
- Communicating or escalating new risks that emerge to their supervisor or manager.

## 8.7   Internal Audit

Internal Audit provides independent, objective assurance and consulting activity designed to add value and improve Council's operations. It helps Council accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal controls, and governance processes.

The Internal Audit Charter defines Internal Audit's purpose, authority, and responsibility.

Internal Audit reports are reported to MANEX and the ARIC to ensure independent oversight of the effectiveness of controls and any recommendations made for improvement.

## 8.8   Audit Risk and Improvement Committee (ARIC)

The ARIC will be responsible for providing independent assurance to the General Manager and Council that the risk management framework is appropriate and working effectively and provide advice on an annual basis that Council has complied with its risk management requirements. This includes advising whether:

- Council's risk management framework operates effectively and supports the achievement of Council's strategic goals and objectives;
- Council's risk appetite is appropriately reflected in the Council's internal control framework;
- Council is operating within the risk appetite determined by Council;
- Risk management covers all relevant risk categories including strategic, operational, compliance, reputational and reporting risks;
- Council takes an enterprise risk management approach that is fully integrated into all aspects of the Council, including decision-making processes and operations;
- Risks are formally considered when developing and implementing all Council policies, programs, projects and other activities, including procurement;
- Major risks have been identified and assessed by Council and appropriate controls have been implemented that reflect Council's risk criteria;
- Internal controls are effective and appropriate;
- Council's risk management framework complies with AS ISO 31000:2018;
- Resources provided for risk management are sufficient for managing the risks facing Council; and
- Risk management policies, procedures and plans are being complied with.

# 9 LEGISLATION AND SUPPORTING DOCUMENTS

## 9.1 Relevant Legislation, Regulations and Industry Standards

- This Policy and Council's risk management approach are informed by the Risk Management Guidelines (AS ISO 31000:2018) issued by Standards Australia.
- Section 428B of the *Local Government Act 1993* (the Act), when proclaimed, along with any subsequent regulations in the *Local Government (General) Regulations 2005* and subsequent Office of Local Government Risk Management Guidelines.

## 9.2 Relevant Council Policies and Procedures

Risk management is a fundamental component of decision making in all Council activities. As such, all policies and procedures (and Council Business Paper Reports, where applicable) should be guided by this Policy and the Risk Management Plan to maintain appropriate risk management considerations at the heart of all decisions and processes.

# 10 VARIATION AND REVIEW

The Risk Management Policy will be reviewed every three (3) years, or earlier if deemed necessary, to ensure that it meets the requirements of legislation and the needs of Council. The term of the Policy does not expire on the review date, but will continue in force until superseded, rescinded or varied either by legislation or a new resolution of Council.

# 11 APPENDIX A

## 11.1 Document Control Continued

| PREVIOUS VERSIONS: | DATE: | RESOLUTION NO: | DESCRIPTION OF AMENDMENTS: | AUTHOR / EDITOR: | REVIEW / SIGN OFF: |
|---|---|---|---|---|---|
| 3 | 22/10/2015 | 14.10/15 | The only amendment was the addition of an Implementation / Communication section, in line with all revised policies. | MRC | Council |
| 2 | 24/10/2013 | 12.10/13 | Minor amendments to spelling and grammar, updating relevant legislation and some minor changes to the current *Risk Management Policy*. The small changes made are in line with better practice protocols to improve the scope of the policy. | MCS | Council |
| 1 | 20/04/2006 | 4.04/06 | First Version created because of the requirements from the then Department of Local Government's 'Local Government Reform Better Practice Review Checklist'. | WHS | Council |