ENTERPRISE RISK MANAGEMENT PROCEDURE

1. Scope

The Enterprise Risk Management Procedure (this 'Procedure') applies to all activities undertaken by Councillors, employees, contractors and volunteers engaged within the provision of Council services.

2. Purpose

Council recognises that risk management is an integral part of good governance and assists in the achievement of objectives, improves service delivery, and drives accountability into decision making.

Council has established this Procedure, in accordance with the Enterprise Risk Management Policy, to provide the necessary guidance for managing enterprise risk within Council and outlines how risk management principles will be embedded at all levels of the organisation.

3. References (legislation/related documents)

Primary
Enterprise Risk Management Policy

Legislative references
Local Government Act 2009
Local Government Regulations 2012

Related documents
AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
COSO Internal Control – Integrated Framework
Conflict of Interest Directive
Conflict of Interest Procedure
Controls Management and Assurance Procedure
Fraud and Corruption Prevention Policy
Fraud and Corruption Control Procedure
WHS Risk Management Procedure

4. Definitions

To assist in interpretation, the following definitions shall apply:

Council	Livingstone Shire Council.
Employees	Local government employee: (a) The Chief Executive Officer; or (b) A person holding an appointment under section 196 of the *Local Government Act 2009.*
Enterprise Risk Management	Enterprise risk management encompasses all the major risk categories (risk impact areas) and includes the coordination, integration, consolidation, and consistency of reporting by the various Council functions with identified risks.

Hazard	A hazard is any source of potential damage, harm or adverse health effects on something or someone.
Internal Controls	'Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance'. - COSO Framework
Mitigation Strength	A judgement of the contribution made by each control to mitigating the risk.
Opportunity	A possible action that can be taken. A favourable or advantageous circumstance or combination of circumstances.
Overall Effectiveness	A yes/no judgement on whether the planned controls are sufficient to mitigate the risk to an acceptable level.
Risk	Effect of uncertainty on objectives. The level of risk is expressed in terms of the combination of consequences and their likelihood.
Risk Appetite	The amount of risk that Council is willing to take in pursuit of achieving its business objectives.
Risk Capacity	The maximum amount of risk that Council can take and remain viable. (Capacity is not a "single number"; it will vary across risk types, business units and strategic scenarios. Discussing capacity is a useful activity in considering how Council could fail).
Risk Management	Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by Council. Managing risk is achieved through the systematic application of policies, procedure, and practices to identify, analyse, evaluate, treat, monitor, and communicate risk.
Risk Owner	The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them.
Risk Register	A list of identified and assessed risks directly related to either a particular department of Council or the whole of Council. Risk registers can be held at either Corporate, Operational, Project or Event level.
Risk Targets	The optimum level of risk, by risk or risk category (risk impact area).
Risk Tolerance	The amount of risk Councill is willing to tolerate. (Commonly quantitative in nature, risk tolerances are thresholds to guide Officers when considering risks, so that they understand the levels that should not be exceeded, or those thresholds that if breached require further mitigation and monitoring).

5. Procedure

To manage risk, Council applies a risk assessment methodology that is designed to ensure that risk management decision making is based on a sound approach, consistency in assessment and utilises a common language that is readily understood across the whole of Council. The approach considers the unique environment in which Council operates.

Note: Council has a supplementary procedure, 'WHS Risk Management Procedure', which forms part of Council's Safety Management System, and should be referred to for guidance on managing workplace health and safety related risks and hazards.

5.1 Roles and Responsibilities

Council

- Review and approve policies presented to Council;
- Consider risk information provided by employees to inform Council decision making;
- Make enquiries to gain satisfaction that risks are identified, managed and controlled appropriately to achieve Council's Strategic Objectives;
- Provide adequate resources and appoint sufficient members to the Audit Risk & Improvement Committee;
- Provide adequate budgetary provision for the financing of risk management including approved risk mitigation activities; and
- Review Council's risk appetite.

In addition, the Mayor is responsible for reviewing and signing the required certificate for the Financial Statements.

Chief Executive Officer

- Establish and maintain a culture of risk awareness and intelligence;
- Ensure governance mechanisms effectively monitor risks and the way they are managed;
- Support Managers in addressing any instances of control breakdown;
- Ensure employees receive support in fulfilling their responsibilities;
- Set standards of best practice for risk management, based on the AS/NZS ISO 31000:2009;
- Manage risks that may impact on Council's ability to achieve the objectives of Council's Corporate Plan; and
- Review and sign the required certificate for the financial statements.

Chief Financial Officer

- Provide advice and support regarding the operation of internal controls relevant to the financial statements;
- Compile the quarterly assurance statements and prepare a summary for the Executive Leadership Team and the Chief Executive Officer; and
- Provide the strategic and functional oversight of the risk management framework.

Executive Leadership Team

- Implement the risk management framework;
- Ensure that regular risk assessments are undertaken within the area of their responsibilities to identify existing or potential risk and ensure that appropriate controls are implemented and functioning appropriately;
- Manage risks that may impact on the department's ability to achieve the objectives of Council's Corporate and Operational Plans;
- Report risks, as required, to Council and the Audit, Risk & Improvement Committee (ARaIC) in consultation with the Chief Executive Officer;
- Maintain awareness of, and assist with the ongoing effective operation of corporate controls; and
- Review and sign off on complete quarterly assurance statements.

Managers

- Manage risks that may impact on the team's ability to achieve the objectives of Council's Operational Plan;
- Provide oversight of the operational risks, including review and maintenance of the risk register, and review of the adequacy and effectiveness of controls and treatments;
- Escalate operational risks that are high or extreme or cannot be managed locally (including risks that require coordination between areas) to the Executive Leadership Team;
- Maintain awareness of, and assist with the ongoing effective operation of corporate controls; and
- Complete quarterly assurance statements as per the requirements of this Procedure.

Risk & Governance Officer

- Provide advice and support to management regarding risk and internal controls;
- Provide training to new Managers on the enterprise risk management framework;
- Maintain the Strategic and Operational risk registers;
- Administrate user management within Council's risk management software and provide training to users;
- Prepare risk reports for the ARaIC, Executive Leadership Team, Council, and other audiences as appropriate;
- Coordinate reviews of Council's risk profile and enterprise risk management framework to reflect currency of position; and
- Monitor application and embedding of the enterprise risk management framework across Council to evaluate its effectiveness.

Although the officer may suggest additional risks and controls, they are not responsible for decisions to implement suggested or other controls, nor are they responsible for the adequacy of risks identified or internal controls for a function.

Employees

All employees, including those with additional responsibilities listed below, are required to support Councils risk management framework:

- Develop a sufficient understanding of Council's policies and other supporting procedures, directives and processes;
- Take direction from management regarding processes and internal controls;
- Act in accordance with the processes and internal controls established;
- Raise additional risks for consideration by their supervisor; and
- Raise any concerns regarding the adequacy of controls.

Project Managers

- Identify risks that may impact on the projects ability to achieve the objectives of the Project Plan;
- Participate and/or facilitate Project Risk Identification Workshops as required;
- Identify, implement, and monitor risk mitigation strategies, controls and treatment actions;
- Maintain Project Risk Register;
- Report and escalate project risks and controls to the Project Control Group for monitoring and oversight; and
- Communicate risks with respective contractors, subcontractors and other stakeholders.

Project Control Group

- Monitor project risks as identified within the Project Risk Register and/or identified emerging risks;
- Monitor status of risk controls and treatment actions; and
- Participate in Project Risk Identification Workshops as required;

Audit, Risk and Improvement Committee (ARaIC)

- Review adequacy and effectiveness of Councils risk management framework and make recommendation to Council as to such appropriateness;
- Provide oversight of the risk management and internal audit functions of Council;
- Review and monitor the development and implementation of risk management principles across Council;
- Monitor changes to Council's risk profile and highlight material changes to Council;
- Monitor performance of implementing action plans arising from risk assessments;
- Review/monitor the documentation of all policies and procedures;
- Oversee management's efforts to create and maintain a strong internal control environment, including the design and implementation of antifraud strategies and programs; and
- Oversee how management is monitoring the effectiveness of its compliance program.

Internal Audit

- Provide advice and support to management regarding risk and internal controls;
- Contribute to the training of employees specifically around internal controls;
- Ensure the Internal Audit Plan gives due consideration to Council's risk registers; and
- Complete reviews on the Internal Audit Plan in a manner that provides evidence-based opinions on the adequacy of controls within the scope of the review.

Although the Internal Auditor may suggest additional risks and controls, they are not responsible for decisions to implement suggested or other controls, nor are they responsible for the adequacy of risks or internal controls identified by management.

5.2 Risk Management Process

Council has adopted a Risk Management Process which aligns to the ISO 31000:2009 Risk Management – Principles and Guidelines and applies a six (6) step process for risk management. See diagram below.

STEP 1: Establish Context

Establish the context by identifying priorities within Councils risk environment. In establishing the context, consideration should be given to:

- Defining the priorities to be achieved;
- The threats that might affect the achievement of priorities;
- The strengths and weaknesses of Council operations;
- Identifying the risk category (Risk Impact Area) and the responsible owner; and
- Identifying relevant stakeholders.

STEP 2: Risk Assessment

Risk Identification

Risk identification involves a wide-range analysis of things that could stop Council from achieving its priorities. Identification of risks generate a comprehensive list of threats and opportunities based on events that may impact on Council and considers risks associated with Council taking or not taking action.

The source of enterprise risks, within strategic and operational levels are categorised into the following Risk Impact Areas:

Impact Area	Description
Assets & Infrastructure (Water, sewerage & waste)	Critical buildings, facilities, equipment, utilities, or physical security on premises. Generally, these assets are associated with water, sewerage and waste, transport and Tier 1 and 2 Council fixed infrastructure as identified through business impact assessments (as defined within Council's Business Continuity Sub-Plans). Essentially these are the assets that underpin our community and on which we rely on for our everyday business and lives. These assets, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social and economic wellbeing of Livingstone's community.
Digital Assets, Systems, Data & Cyber Security	Critical digital assets, technology, telecommunications and information are impacted by a specific threat.
Economic	Risks arising from uncertainty about economic outcomes such as production, consumption, and distribution of goods and services.
Environmental	Adverse impacts on the climate, the sustainable use of natural resources, biodiversity and ecosystems.
Financial	Financial or quantifiable impact due to loss of revenue, increased costs or damage to property or equipment.
Governance (Legal, Compliance and Regulatory)	Non-compliance with regulatory requirements, inability to fulfil contractual obligations leading to penalties or sanctions.
Reputation	Council's reputation and image is adversely impacted and may lead to adverse coverage on various media platforms due to delay or unavailability of key products or services. Refers to the chance of losses due to a declining reputation as a result of practices or incidents that are perceived as dishonest, disrespectful or incompetent. May also refer to a serious loss of confidence in Council rather that a minor decline in reputation.

People	Human factors such as talent attraction, retention and engagement, workforce exhaustion, inadequacies in human capital and the management of human resources.
Service Delivery	The critical business functions and/or day-to-day operations of Council are impacted.
Workplace Health & Safety	The possibility that harm (death, injury or illness) might occur when exposed to a hazard in the workplace.

The following information, sources and methods also help to identify risks:

- Reviewing hazard logs, incident reports, customer feedback and complaints, insurance claims, and survey reports;
- Reviewing audit reports such as financial audit reports and internal audits, or workplace health & safety reports;
- Strength, weaknesses, opportunities and threats (SWOT) analysis, or a Project Risk Identification Workshop; and
- Benchmarking against other organisations.

Risk Analysis

This stage includes the undertaking of a Risk Assessment to analyse the identified risks. The assessment will analyse the likelihood of a risk occurring and the consequences if it does occur. The Risk Rating Matrix (***Appendix 1***) and the Risk Likelihood Table (***Appendix 2***) provides guidance to determine the likelihood of a particular outcome. The Risk Consequence Table (***Appendix 3***) is also used for this process as it helps determine the consequence (risk impact) to Council. When analysing the risks critical judgment should be used to determine what is appropriate and reasonable.

*Note: Risk assessments can either be performed directly within Council's Risk Register, or via a Risk Assessment Template (**Appendix 5)**, and then transferred into the risk register thereafter.*

Risk Evaluation

The evaluation considers the controls currently in place and whether the existing controls are sufficient, or whether additional controls must be identified and implemented to further mitigate the risk to Council.

Risk treatment and control is designed to either reduce the likelihood of the risk occurring or to reduce the consequences of the risk were it to occur.

If the circumstance arises that, even with proposed additional treatments, the assessed risk level will remain at an unacceptable level, serious consideration should be given as to whether the activity, that will create the risk, is to be commenced or continued. However, it should not be assumed that the activity must cease.

STEP 3: Risk Treatment (additional controls)

Once the risk context has been established and the risks have been assessed, efficient and effective controls and actions must be determined. Controls and actions should help mitigate the risk or strengthen current controls. Defining controls vs actions is outlined below:

- **Controls** are an existing strategy used to maintain or modify a risk and may include any process, policy or practice and are an ongoing function of the business.
- **Actions** are a new planned, temporary strategy applied to maintain or achieve the target level of risk after controls are applied. Actions are undertaken in a pre-determined timeframe.

NOTE: An **action can transition to a control** if the strategy becomes an ongoing function.

Risk Control Effectiveness: This term is used to describe how well a control is reducing or managing the risk it's meant to modify. The more effective a control is, the more confidence Council has that the risk is being managed as expected.

Council applies the following three-level scale to define the level of control effectiveness:

Effectiveness Level	Definition/ Performance
Effective	Controls eliminate or remove the source/root cause of the risk; or Controls are well documented, consistently implemented and reliable in addressing the source/root cause of risk. High degree of confidence from management in the protection provided by the controls.
Partially Effective	Controls are in place buy may be partially documented or communicated, or inconsistently applied or infrequently tested. Weaknesses in the controls are minor or moderate and tend to reflect opportunities for improvement, rather than serious deficiencies in system or practices.
Ineffective	Controls aren't documented or communicated or are inconsistently implemented in practice. The controls aren't operating as intended and risk isn't being managed. Controls aren't in place to address the root cause/ source of risk.

Risks that do not have sufficient controls in place to effectively manage the risk to Council in accordance with its defined risk appetite, must consider the most appropriate risk mitigation strategy. The four (4) main risk response strategies are outlined below:

Strategy	Definition
Accept	No action taken; risk is acceptable.
Avoid	Action taken to do something different because of the existing risk, so the risk is eliminated.
Transfer	Action taken to decrease risk severity by either implementing controls or sharing risk. I.e., Insurance.
Reduce (mitigate)	Action taken to reduce the probability or impact of risk.

Note: To determine whether a risk is within Council's risk appetite refer to Councils Risk Appetite Statement as outlined within the Enterprise Risk Management Policy.

Treatments need to be appropriate to the significance and priority of the residual risk, and should consider the following:

- Cost benefit analysis of each option including the cost of implementation;
- Any legal, regulatory or other requirements which may exist;
- Council's risk appetite;
- Any political, social and environmental factors that may be relevant to a risk treatment;
- Use of proven risk controls;
- Any risks which the treatment itself may cause or introduce;
- Impact of treatment on stakeholders and/or stakeholder expectations on how the risk should be treated; and
- The anticipated level of risk remaining after implementation of risk treatment.

Once treatment options for individual risks have been identified, they are assembled into a Risk Treatment Plan (***Appendix 6***). The purpose of the Risk Treatment Plan is to document how the chosen treatment options will be implemented.

Acceptance of Risk Treatment Plan's and associated actions will be determined in accordance with the Risk Tolerance & Action Table (***Appendix 4***). In considering and applying risk treatment strategies, there must be an awareness of any new risks created by the treatment. These new risks must be assessed and managed appropriately.

When implementing identified control measures, all persons that may be affected need to be informed of these measures.

STEP 4: Monitoring and Review

Continuous monitoring and review of risks, associated controls and treatment plans is an essential part of the risk management process. This stage determines whether:

a) The identified risks still exist;
b) New/associated risks have emerged;
c) The likelihood or consequences of risks have changed;
d) The controls and treatment strategies/actions have been or continue to be effective; and
e) Further controls are required to be implemented or if some controls can be retired or replaced with alternatives.

Risk reviews should also be undertaken before a change in the workplace environment or processes, and/or as results of consultation indicate that a review is necessary.

The risk owner will be required to determine an approach to monitoring the risk, however, '**Appendix 4 – Risk Tolerance & Action Table (generic)'** is a matrix to guide monitoring and review dates against residual risk ratings.

Monitoring and reviewing risk management activities allows Council to analyse and learn lessons from successes and/or failures.

Monitoring and reviewing activities occur through, but are not limited to:

- Internal review program, including discussion in team meetings;
- Internal audit and external audit;
- External scrutiny (appeal tribunal, courts, commission of inquiry);
- Physical inspection;
- Program evaluation;
- Reviews of organisational policies, strategies and processes; and
- Consideration of risks within all Council reports (mandated in template) including projects.

STEP 5: Communication and Consultation

Communication, consultation and feedback take place during all steps of the enterprise risk management process. Methods of the communication, consultation and feedback will be dependent upon the nature of the risk, and on the stakeholder/s with whom the communication, consultation and feedback need to occur. Effective communication, consultation and feedback will ensure that:

- Important risks are not overlooked;
- Risks are accurately defined;
- Risk assessments are realistic; and
- Reduced levels of resistance are encountered when implementing risk treatments.

STEP 6: Recording and Reporting

Each stage of the risk management process must be recorded to ensure:

- There is sufficient information to demonstrate how risks have been managed using the

enterprise risk management framework. This is guided by the mandatory fields to be populated in the risk register;

- Decisions to treat or not to treat risks are clearly supported; and
- Key information is readily accessible and reporting risk to management and stakeholders is targeted and insightful.

Reporting of risks will occur through:

a) Regular risk management reports to the Audit, Risk and Improvement Committee (biannual at minimum), including information in the areas of enterprise risk management, business continuity planning, fraud and corruption, insurance, and workplace health and safety;

b) Annual reporting and presentation of Operational Risk Registers (by portfolio) to the Audit, Risk and Improvement Committee;

c) Adhoc reporting of high risks to the Audit, Risk and Improvement Committee.

d) Risk reporting to the Executive Leadership Team on a quarterly basis (following quarterly risk reviews by risk owners);

e) Monthly reporting to the Executive Leadership Team for Extreme/High risks and/or risks that are significantly outside Council's defined tolerance level/appetite;

f) Annual review of the Corporate Risk Register by the Executive Leadership Team; and

g) Risks reported to Council via Council Meeting Reports.

5.2.1 Council Reports (Council decision-making process)

Council reports are required to include an analysis of risks relevant to the matter to provide supporting information to Council for decision-making.

Where a report requires a decision by Council, the report should include either:

A) A **detailed risk assessment** (completed risk assessment form which outlines identified risks, opportunities, and associated mitigation strategies with applied risk ratings) attached to the Council Report.

The 'Risk Assessment' section of the Council Report will refer to the attached risk assessment and therefore only requires a high-level summary within the body of the report to confirm that:

- That associated risks and opportunities have been identified; and
- The identified risks and opportunities align with Council's defined Risk Appetite and supports the report Recommendation.

EXAMPLE: 'Officers have assessed the associated risks (as outlined within the attachment) of this initiative and is *within/outside of* Council's defined risk appetite for *financial *(*applicable risk impact area)* risks'. **

**Officers may even choose to include an extract from Council's Risk Appetite Statement ('will/will not tolerate' statements) to support the recommendation.

B) A **risk assessment summary** that identifies risks and mitigation strategies relative to the report matter (that are documented as a high-level summary within the report, rather than attached as a detailed assessment with applied risk ratings).

Note: alignment to Council's defined risk appetite is still required.

EXAMPLE: The identified risks associated with this initiative have been assessed and align with Council's defined risk appetite. Key areas of consideration include:

- **Operational Risks**: Potential disruptions to service delivery during implementation have been evaluated. Mitigation measures include robust project management, resource allocation, and contingency planning to ensure minimal impact on operations.

- **Financial Risks**: Cost overruns or unexpected expenses could affect the project budget. These risks are managed through detailed financial forecasting, regular budget reviews, and alignment with Council's financial governance practices.
- **Reputational Risks**: Public perception challenges or stakeholder dissatisfaction have been identified as moderate risks. Proactive engagement and clear communication strategies are in place to maintain transparency and trust with the community and stakeholders.

All residual risks fall within the thresholds defined by the Council's risk appetite. Ongoing monitoring and adaptive strategies will ensure compliance with Council's enterprise risk management framework and support the initiative's successful delivery'.

Where the report is for Councillor information only, the report author may choose not to include a detailed risk assessment however the 'Risk Assessment' section of the Council Report must provide a statement to confirm that the officer has considered the matter (with context of information provision) and has not identified any associated risks.

If risks have been identified, these must be included within the report, either as a high-level summary or attached as a detailed risk assessment. This statement may also reference how the reporting of this information assists Council to manage risks.

EXAMPLE: 'This report has been prepared for Councillor information only and has not identified any risks associated with the provision or reporting of this information. By providing clear and accurate data, the report supports Council's ability to manage risks effectively by enabling informed decision making and promoting transparency.

The reporting process aligns with Council's commitment to proactive risk management, ensuring that risks are identified, monitored, and addressed'.

5.3 Enterprise Risk Management Tools

Monitoring and reporting risks requires the use of various tools and methods to collect, store, process and present data. This section outlines a diverse list of tools utilised by Council.

5.3.1 Risk Registers

The Risk Register sets out the identified risks (including the material risks), impact, risk assessment, existing controls, residual risk, proposed treatment, responsible manager and the sources of assurance.

The corporate system used to record Strategic and Operational risks is Pulse, and Project Focus HQ for project risks.

5.3.2 Risk Identification & Assessment Tools

Council has a number of Risk Management Tools to assist in identifying, assessing and controlling hazards and risks. These include:

- Workplace Inspections – a site-specific checklist used to identify hazards within a building or worksite;
- Risk Assessment Form – a risk assessment template to assist identify hazards, assess risks and implement controls for a particular task;
- Pre-Start Daily Risk Assessments – a generic risk assessment used at the start of each day for construction work to identify hazards, assess risks and ensure adequate controls are in place;
- Safe Work Method Statements – risk assessments developed for high-risk construction work;
- Project Risk Identification Workshops (with Project Manager and Project Control Group);
- Annual Operation Risk Review Workshops (with Business Unit/Portfolio Managers

and Executive Leadership Team); and

- Strategic Risk Profile Review Workshops (with Executive Leadership Team and Councillors).

5.3.3 Risk Treatment Plan

A Risk Treatment Plan is used to help work through the treatment decision making process in a structured manner. The Plan also helps schedule actionable priorities and progress against the Plan can be monitored.

5.4 Integration of Enterprise Risk Management

Enterprise risk management is integrated into Council's philosophy and organisational culture through:

a) A whole of Council focus on risk management, where Councillors, the Executive Leadership Team, Managers and employees come together to discuss risk management issues. This occurs through, but are not limited to:

- Council reports and Council workshop discussions;
- Executive Leadership Team meetings;
- Leadership Team meetings; and
- Team meetings/ Toolbox talks.

b) Direction on risk management expectations is articulated throughout Council including Council's risk appetite and providing tools and processes to be followed to ensure effective risk management.

c) Risk management is a central consideration in all decision-making processes. Where reports or briefing papers are prepared for decision makers, risks are clearly identified, and mitigation actions are recorded where appropriate. Risk management is also a key consideration in project and event management, and business cases.

d) Council invests time and resources, including financial resources, in regular training and information sessions for all Councillors and employees to ensure awareness of Council's expectations. Council is committed to a shared language and understanding of risk management, ensuring that there is a common understanding of risk management principles and building the overall capability and capacity of employees in relation to risk management.

5.5 Training

To ensure the successful implementation of risk management throughout Council, appropriate training in risk management will be provided.

Council will ensure that all employees receive risk management training and information as outlined below:

- Induction (Employee/Councillor/Contractor/Volunteer)
- Pulse Software | Project Focus HQ Training (Supervisors/Coordinators/Managers/ELT)

5.6 Conflicts of Interest

Council recognises that from time-to-time conflicts may occur concerning the need to reduce a risk versus the community good. These conflicts may be unexpected.

To mitigate conflicts of interest in risk management, it's crucial to promote and foster a culture of integrity within the organisation. This involves setting clear ethical standards, ensuring transparency in decision-making processes, and encouraging open communication about potential conflicts. Council's Conflicts of Interest Policy and Procedure prescribes how such conflicts are to be managed.

6. Changes to this Procedure

This Procedure is to remain in force until otherwise amended/replaced or other circumstances arise.

7. Repeals/Amendments

This Procedure repeals the Livingstone Shire Council Procedure titled 'Enterprise Risk Management Procedure (v2.1) and the Enterprise Risk Management Framework (v2)'.

Version	Date	Action
1.0	22/09/2015	Approved
2.0	09/10/2017	Amended Procedure Approved
2.1	04/01/2019	Administrative Amendments – reflect organisational restructure and update approving officer to Chief Executive Officer
3.0	13/12/2024	Amended Procedure Approved – full review undertaken and procedure amended

ANDREA ELLIS
CHIEF FINANCIAL OFFICER

Appendix 1 - Risk Rating Matrix

The overall risk rating is determined by finding the point of intersection between the likelihood rating (vertical axis) and the consequence rating (horizontal axis).

Likelihood	Consequence: Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Low	Medium	High	High
Unlikely	Insignificant	Low	Low	Medium	High
Rare	Insignificant	Insignificant	Low	Low	Medium

*Refer to Councils Risk Appetite Statement, as annexed to the Enterprise Risk Management Policy to determine Council's appetite for risk against specific risk impact areas to determine the level of mitigation and reporting required.

Note: Workplace health and safety utilise the same 5x5 matrix, with the inclusion of a numbering system to provide further guidance in alignment with Council's Safety Management System. Refer to the WHS Risk Management Procedure.

Using the Risk Rating Matrix

The risk rating matrix is a tool designed to help analyse risks and prioritise them for treatment and reporting. It reflects the materiality of a risk in accordance with pre-defined consequence and likelihood criteria that are aligned to the categories of risk. The matrix is positioned at a Council-wide level to maintain a consistent perspective of risk management across all staff and portfolios.

To use this matrix, identify which category (Risk Impact Area) the risk falls into and the estimated impact should the risk become an event. After the controls have been identified, estimate the likelihood of the risk occurring, this will identify the Risk Rating.

NOTE: The Risk Rating Matrix has been built into the Pulse software, which will automatically calculate and apply a risk rating once the risk consequence and risk likelihood is selected.

Appendix 2 – Risk Likelihood Table

The likelihood rating refers to the potential for the risk to happen, measured by probability and frequency. The likelihood that an event will occur is not always easy to assess. Subjective biases may give rise to different assessments by different people. To avoid this situation, and in order to provide a degree of consistency across the organisation in assessing likelihood, the following table is to be used as a guide.

	All 'Risk Impact Areas', but excluding WHS	
Likelihood Category	**Probability (The risk has occurred, or it is probable that it will occur)**	**Description**
Almost Certain	More than 1 event per year > 90%	Expected to occur; frequent similar occurrences in local government/Council history.
Likely	More than 1 event over 1 to 2 years 60%-90%	Strong possibility to occur occasionally; similar occurrences known often in local government/Council history.
Possible	Once every 2 to 10 years 40%-59%	Might occur, capable of happening, foreseeable; similar occurrences experienced in local government/Council history.
Unlikely	Once every 10 to 100 years 10%-39%	Not likely or expected to occur; rare but not unheard-of occurrence in local government/ Council history.
Rare	Less than once every 100 years <10%	Very unlikely to occur; no recent similar instances in local government/ Council history.

Appendix 3 – Risk Consequence Table

RISK IMPACT AREA	LEVEL OF IMPACT					
	Insignificant	Minor	Moderate	Major	Catastrophic
Financial	Negligible financial loss or overspend; less than <$100,000.	Minor financial loss or overspend; >$100k-<$250k	Significant financial loss or overspend; >$250K - <$1M	Major financial loss or overspend; >$1M - <$20M	Extensive financial loss or overspend; >$20M
Economic	None to minimal impact or inconvenience to single businesses within the Council area.	Inconvenience to a group of businesses within one sector or locally within the Council area.	Group of businesses in one sector or locally within the Council area put at risk.	A minor industry or whole sector of Council area economy put at risk.	One or more major industries (e.g. Tourism, Agriculture, Education, Construction, Manufacturing, and Retail,) within the Council area are threatened.
Digital Assets, Systems, Data & Cyber Security	Critical assets/ systems/ information are unavailable for a very short time period, causing negligible negative impact on Council's business operations.	Critical assets/ systems/ information are unavailable for a short time period, causing minor negative impact on Council's business operations. (Up to 48hrs)	Critical assets/ systems/ information are unavailable for a moderate time period, causing partial negative impact on Council's business operations. (2-7 days).	Critical assets/ systems/ information are unavailable for a long time period, causing significant negative impact on Council's business operations. (7-14 days)	Critical assets/ systems/ information are unavailable for an extended time period causing severe and irreversible negative impact on Council's business operations. (>14 days)
Assets & Infrastructure (Water, sewerage & waste)	Damage where repairs are required however still operational. **Water & Sewer:** Damage or failure not impacting services to more than one household.	Minor loss/damage. Repairs required. (>24hrs *critical assets/infrastructure). **Water & Sewer:** Damage or short-term failure impacting multiple households <24 hours.	Short to medium term loss of key assets & infrastructure. (1-2 days *critical assets/infrastructure). **Water & Sewer:** Damage or short to medium-term failure impacting multiple households <48 hours.	Widespread, short to medium term loss of key assets and infrastructure. (>2 days *critical assets/infrastructure). **Water & Sewer:** Damage or medium-term failure impacting multiple households <7 days or water quality incident per DWQMP or SCADA outage >4 hours.	Widespread, long-term loss of substantial key assets and infrastructure. (>5 days *critical assets/infrastructure). **Water & Sewer:** Damage or long-term failure impacting multiple households >7 days.
People	Minimal HR issues easily remedied. High level of staff productivity despite risk. No impact on staff turnover.	Some HR issues within organisation, staff turnover considered appropriate. Appropriate level of productivity remains despite identified risk. Minor impact on staff turnover (>10% turnover *excl. end of fixed term/retirements).	Elements of poor HR culture, above average staff turnover and reduced long term productivity due to HR issues. Moderate impact on staff turnover (10-15% turnover)	Poor internal culture within various departments hampering innovation and achievement, high staff turn-over and ongoing loss of valued employees. Attracting poor prospective employee candidates. High level reduced productivity due to HR issues. Major impact on staff turnover (15-20% turnover).	Organisational wide poor internal culture hampering innovation and achievement, high staff turn-over and ongoing loss of valued employees. Attracting poor prospective employee candidates. Severe reduced long-term productivity issues resulting from HR issues. Severe impact on staff turnover (>20% turnover).
Governance (Legal, Compliance and Regulatory)	Dispute resolved through internal process or expertise. LEGAL: Threat of litigation requiring small compensation. CONTRACT: No effect on contract performance.	Dispute resolved through legal advice. LEGAL: Single Minor litigation. CONTRACT: Results in meeting between two parties in which contractor expresses concern.	Council directed to undertake specific activities to remedy breaches in legislation that may require the involvement of legal firms. Councillor reprimanded. LEGAL: Single Moderate litigation or Numerous Minor Litigations. CONTRACT: Receive verbal advice that if breaches continue, a default notice may be issued.	Deliberate breach or gross negligence / formal investigations from third party (CCC). Council sanctioned by State Government. Councillors referred to Conduct Review Board. LEGAL: Single Major litigation or numerous Moderate Litigations. CONTRACT: Receive written notice from the contractor threatening termination if not rectified.	Major breach of legislation resulting in major corporation penalties, fines, CCC investigation that may result in legal action against Council staff/Elected Members, or class action. State Government dismisses Council. LEGAL: Numerous Major Litigations. CONTRACT: Termination of Contract for default.
Environmental	Minor environmental incident that can be remedied immediately with no lasting detrimental effect.	Minor/ short term public health or environmental incident (weeks). Response occurs from within existing budget. Penalty and prosecution possible through LSC due to breaches of Council's Local Laws.	**Localised impact.** Medium term major public health or environmental incident (> 3 months), requiring the allocation of some resources to rectify reversible damages. May incur cautionary notice of infringement notice. Penalty and prosecution possible through LSC due to breaches of Council's Local Laws.	**Significant impact locally and potential for offsite impact.** Long term major public health or environmental incident (>1yr), requiring significant resources to respond. High level penalties and prosecution likely through DES due to breaches of the EPA/ prosecution possible through LSC due to breaches of Council's Local Laws.	**Significant impacts to regional ecosystems and threatened species, potential for widespread offsite impacts.** Permanent, major environmental or public health damage, requiring significant resources to respond. High level penalties and prosecution likely through DES due to breaches of the EPA/ prosecution possible through LSC due to breaches of Council's Local Laws.
Workplace Health and Safety	**No injury.** None or very minimal injuries; no first aid required. No damage, environmental or operational impact.	**First Aid Injury.** Minor injuries resulting in first aid treatment only. No disability, no lost employee time.	**Medical Treatment.** Moderate injuries where medical treatment is required. Injury/ies result in work stoppage, no disability. OR would cause several casualties that require hospitalisation with no long-term effects.	**Serious injuries** where short-term hospitalisation is required. Psychological or physical harm to small sector(s)of the community or staff. Serious casualties resulting in the long-term physical impairment of personnel.	**Severe injuries, loss of life.** (Fatality, permanent disability or long-term hospitalisation; Significant psychological or physical harm to considerable sector(s) of the community or staff).
Service Delivery	No impact on Council from achieving any of the key outcomes detailed in the Corporate Plan. No remedial action required. No impact on customers.	May have some effects that prevent Council from achieving any of the key outcomes detailed in the Corporate Plan. Further remedial action required. Moderate impact on customers.	Impacts on Council's delivery of any of the key outcomes detailed in the Corporate Plan. Significant customer impact for up to 48 hours.	Severely impacts Council's delivery of any of the key outcomes detailed in the Corporate Plan. Interruption for 2-7 days.	Prevents Council from achieving any of the key outcomes detailed in the Corporate Plan. Interruption for more than 7 days.
Reputation	External reputation not affected. No effort or expense required to recover.	External reputation minimally affected. Little effort or expense required to recover.	External reputation damaged: some effort and expense required to recover.	External reputation severely damaged: considerable effort and expense required to recover.	External reputation irrevocably destroyed or damaged. Perceived as failing authority requiring intervention.

Appendix 4 – Risk Tolerance & Action Table

Residual Risk Rating	Response Time	Level of Action Required	Responsibility
EXTREME	Immediate action required	**NEEDS IMMEDIATE ACTION:** Unacceptable level of risk. Activity should stop immediately with escalation to ELT. Risk Mitigation Plan to be developed and implemented. Weekly reporting on control effectiveness and mitigation plan by the Risk Owner to ELT. Risk Treatment Plan may be subject to Council approval. *	CEO and ELT
HIGH	Action required as soon as possible	**NEEDS PREVENTATIVE OR CORRECTIVE ACTION WITHIN 1 MONTH:** The risk should be mitigated or avoided, unless the anticipated benefits of the activity outweigh the consequences of the risk. Risk Mitigation Plan to be developed and implemented, with approval by respective Portfolio Manager. Monthly reporting to ELT (by Risk Owner) on control assurance/ mitigation plan. *	Portfolio Manager and ELT
MEDIUM	Action required within routine business schedules	**NEEDS PREVENTATIVE OR CORRECTIVE ACTION WITHIN 3 MONTHS:** The risk may be acceptable with adequate and effective controls, managed by specific procedures and subject to ongoing monitoring. Regular review and reporting, at least quarterly, to be provided within respective business unit and to affected stakeholders.	Manager/Risk Owner
LOW	Immediate action not required	**DOES NOT CURRENTLY REQUIRE PREVENTATIVE OR CORRECTION ACTION:** The risk is generally acceptable but must be monitored to make sure that the risk rating does not change. Risk managed by routine controls and reviewed annually or after significant change.	Manager/Risk Owner
INSIGNIFICANT	Not applicable	The risk is acceptable.	NA

*High & Extreme risks require a risk treatment plan which is reported to the Chief Executive Officer (via the Executive Leadership team) and the Audit, Risk & Improvement Committee.

Note: Refer to the 'Minimum Action Requirement Guide as prescribed within the 'WHS Risk Management Procedure' for action and reporting timeframes relating to WHS risks'.

Appendix 5 – Risk Assessment Form (Template)

RISK ASSESSMENT FORM (Corporate)

Completion Details

Date:	
Completed by:	
BU/Project/Event:	

Risk Rating Matrix

Likelihood \ Consequence	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Low	Medium	High	High
Unlikely	Insignificant	Low	Low	Medium	High
Rare	Insignificant	Insignificant	Low	Low	Medium

*Refer to Council's ERM Procedure for guidance on how to utilise the matrix to formulate a risk rating.

Risk	Cause	Consequences	Inherent Risk			Controls (existing)	Residual Risk			Risk Owner
			Likelihood	Consequence	Rating		Likelihood	Consequence	Rating	

Risk Treatment Plan

Completion Details

Date:	
Completed by:	

Risk Details

Risk:					
Cause | Description:					
Controls (Existing)					
Residual Risk Rating					
Likelihood		Consequence		Rating	

Treatment Plan

#	Action (referred to as a Task within Pulse)	Responsible Officer	Cost*	Timeframe		
				Start	Completion	Duration
1						
2						
3						
4						
5						

*Note: Action/Task 'costs' are not recorded within Pulse, however, are included within the template to ensure consideration is given to evaluating the risk vs the cost of mitigation.