LIVERPOOL
CITY
COUNCIL

ENTERPRISE RISK MANAGEMENT POLICY

Adopted: 28 June 2017

TRIM: 103446.2017

LIVERPOOL
THE GREAT SOUTH WEST

CONTENTS

1. PURPOSE/ OBJECTIVES

1.1 Council understands that large, unmitigated risks can adversely impact upon its stakeholders and its ability to achieve strategic and operational objectives. Accordingly, Council is committed to a systematic, proactive and enterprise wide approach to managing risk.

1.2 The application of ERM thinking, principles and practices aims to help Council deliver quality services, improve decision-making, set priorities for competing demands/ resources, minimise the impact of adversity and loss, ensure regulatory compliance and support the achievement of objectives.

1.3 This policy applies to all Councillors, all members of Council staff and Council contractors, consultants and volunteers across all Council activities and processes.

2. LEGISLATIVE REQUIREMENTS AND APPLICABLE STANDARDS

Australian Standard: AS/NZS ISO 31000:2009
Local Government Act 1993

3. DEFINITIONS

CEO means the Chief Executive Officer.
Council means Liverpool City Council.
ERM means enterprise risk management.
HAR means the Head of Audit and Risk.
Risk is defined as the effect of uncertainty on objectives.

4. POLICY STATEMENT

4.1 Mandate and commitment

Council is committed to the formal, systematic, structured and proactive management of risks across Council. This includes financial, legal, reputational, safety, service delivery and environmental risks.

4.2 ERM framework

4.2.1 Council's ERM is a set of components that aims to provide the foundations and organisational arrangements for designing, implementing, monitoring reviewing and continually improving ERM throughout Council.

4.2.2 Council is committed to maintaining an effective, efficient and tailored ERM framework that consists of:

a) This policy;
b) Council's ERM process (attached to this policy);
c) Supporting policies and processes that complement ERM such as fraud prevention, business continuity management, project management and work health and safety management systems.

4.2.3 The framework should enable:

a) A formal, structured approach to ERM that is appropriate to Council's activities and operating environment; and
b) An ERM approach consistent with the principles of AS/NZS ISO 31000:2009.

4.2.4 This framework should be related to Council's community strategic plan, operational plan and delivery program.

4.3 Risk appetite statement

4.3.1 Risk appetite is the amount of risk that Council is willing to take in pursuit of its objectives. Council's risk appetite may vary depending on the importance and complexity of each objective that Council is pursuing in accordance with the decisions of Council and the particular strategies in place to achieve those objectives which should be related to its current community strategic plan, operational plan and delivery program.

4.3.2 Council acknowledges that there is a certain level of inherent risk in its activities and acknowledges that accepting a certain level of risk helps Council to develop and improve in terms of meeting its strategic objectives. However, in accepting such risks, Council must consider its current financial and staffing capacity and the potential impacts on Council's longer term financial, environmental and social sustainability.

4.3.3 Council has little or no appetite for known and avoidable operational risks that are primarily identifiable in Council's Risk Register and which may adversely affect the safety and wellbeing of members of Council staff and the local community within its Local Government Area, financial viability of Council and the security of Council assets.

4.4 Implementing risk management

Council is committed to ensuring that a strong ERM culture exists within Council and should develop and maintain an ERM process that:

a) Aligns ERM processes to existing planning and operational processes;
b) Allocates sufficient funding and resources to ERM activities;
c) Provides staff with appropriate training in ERM principles;
d) Ensures that Internal Audit, directors and managers assign clear responsibilities to Council staff at all levels for managing risk;
e) Embeds key controls to manage risks into business processes;
f) Establishes appropriate mechanisms for measuring and reporting ERM performance;

g) Communicates ERM policies, processes and issues to Council staff, the Audit, Risk and Improvement Committee and other stakeholders;

h) Receives and considers recommendations received from Council staff, the Audit, Risk and Improvement Committee and other stakeholders in relation to Council ERM policies, processes and issues; and

i) Facilitates continual improvement.

4.5 Accountabilities and responsibilities for managing risk

4.5.1 The elected Council is ultimately responsible for:

a) Reviewing, adopting and committing to this policy;

b) Identifying and monitoring emerging risks;

c) Fully considering ERM issues contained in Council reports;

d) Fully considering the risks arising from its decisions;

e) Providing feedback to the CEO on important ERM matters/ issues raised by the CEO;

f) Supporting management in communicating the importance and benefits of good ERM to stakeholders.

4.5.2 The Audit, Risk and Improvement Committee is responsible for :

a) Monitoring the risk exposure of Council by determining if Council has appropriate ERM processes and adequate management information systems in place

b) Establishing and reviewing the framework for identifying, monitoring and managing significant business risks. This includes periodically reviewing Council's ERM Policy and processes;

c) Oversight and monitoring of the implementation of Council's ERM process;

d) Monitoring the implementation of risk treatment plans;

e) Determining whether to accept or further treat residual risks that are assessed as high or above; and

f) Identifying and monitoring emerging risks.

4.5.3 The Chief Executive Officer, with the assistance of the Audit, Risk and Improvement Committee, is responsible for leading the development of an enterprise ERM culture across Council and ensuring that this policy and process are effectively implemented. The CEO is especially responsible for:

a) Where appropriate, reporting known potential risks, emerging risks or major incidents to Council in a timely manner;

b) Determining whether to accept or further treat residual risks that are assessed as high or above;

c) Ensuring that ERM activities are aligned to Council's process and objectives; and

d) Ensuring sufficient funds are available to support effective and efficient management of risks.

4.5.4 Directors are responsible for ensuring that this policy and process are effectively implemented within their directorate and for determining whether to accept or further treat residual risks that are assessed as medium.

4.5.5 Managers are the risk owners for the purpose of this policy and process. They are required to create an environment where the management of risk is accepted as the personal responsibility of all members of Council staff and Council volunteers, consultants and contractors. All managers are accountable for the implementation and maintenance of sound ERM processes and structures within their area of responsibility in conformity with Council's ERM framework, including:

a) Identifying, recording and periodically evaluating risks;
b) Identifying, recording and assessing effectiveness of existing controls;
c) Implementing and maintaining effective internal controls;
d) Developing treatment plans to treat higher level risks in a timely manner;
e) Maintaining up to date risk registers through quarterly reviews and updates;
f) Complying with and monitoring Council staff compliance with Council's policies and processes;
g) Maintaining up to date information and documentation for key operational processes; and
h) Ensuring ERM plans are added Council's operational plan and budget, as required.

4.5.6 The Head of Audit and Risk (HAR) is responsible for coordinating processes for ERM throughout Council, including the provision of advice and service assistance on ERM issues.

4.5.7 All members of Council staff and Council contractors, consultants and volunteers must act at all times in a manner which does not place at risk the work health and safety of themselves or any other person in the workplace. Members of Council staff are responsible and accountable for taking practical steps to minimise Council's exposure to risks insofar as is reasonably practicable within their area of activity and responsibility.

All members of Council staff must be aware of operational and business risks, in particular, they should:

a) Provide input into various ERM activities;
b) Assist in identifying risks and controls;
c) Report all emerging risks, issues and incidents to their supervisor or a responsible member of Council staff;
d) Follow Council policies and processes.

5. FRAMEWORK

5.1 General

5.1.1 Council's ERM framework provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving ERM throughout Council. The key elements of Council's framework is this policy which:

a) Establishes a mandate and commitment for managing risk;

b) Sets out the means by which ERM should be implemented within Council through processes, practices, assignment of responsibilities, sequence and timing of activities to help Council staff manage risk.

5.1.2 Council appreciates the importance of an effective ERM framework to help protect key stakeholders from adverse events and support the pursuit of opportunity. Council aims to maintain an ERM framework appropriate to the size, culture and complexity of its operations and environment.

5.1.3 Council has an ERM framework in place, based on Australian Standard AS/NZS ISO 31000:2009 Risk management. Council seeks to embed the ERM framework is within Council's overall strategic and operational policies and practices. This policy and Council's Risk Register are key components of the framework.

5.2 The ERM process

5.2.1 The ERM process can be applied to a particular activity, service, process and project, and to part or the whole of Council operations.

5.2.3 This process also aims to ensure a consistent, proactive and holistic approach that encourages a "whole of business" or "enterprise-wide" view of risk rather than managing risk in "silos".

5.3 Benefits of managing risk

5.3.1 The benefits of a risk aware culture, regular ERM thinking and managing Council-wide risks include:

a) Increased likelihood of achieving objectives;
b) Better decision-making and planning;
c) Better identification of opportunities and threats;
d) Proactive rather than reactive management;
e) More effective allocation and use of resources (human, financial, intellectual);
f) Improved stakeholder confidence and trust;
g) Improved compliance with key regulatory requirements;
h) Improved internal control environment;
i) Better corporate governance; and
j) Enhanced communication and reporting of risk.

5.4 ERM parameters

5.4.1 Risk parameters are generally expressed in terms of risk appetite and risk tolerance.

5.4.2 Risk appetite is the amount of risk that Council is should take and accept in pursuit of its objectives. It is Council's "comfort zone". It is about knowing where to draw the line between acceptable risks and unacceptable risks and identifying the level of additional controls required. Understanding risk appetite is particularly relevant when Council has to make decisions that are inherently uncertain.

5.4.3 Council has little or no appetite for known and avoidable operational risks that might impact on the safety and wellbeing of staff and the community, security of Council and public assets, Council's reputation and/ or the delivery of quality services to the community. Council acknowledges that it should have to take some calculated risks in order to achieve its strategic objectives. However, in taking such risks Council must consider current financial and human capacity and the potential impact on longer term financial, environmental and social sustainability.

5.4.4 Risk tolerance is the amount of risk Council is should bear in respect of a particular function, activity or risk type. Ideally, the tolerance is quantified, but in any event is expressed so that relevant management responsibilities are absolutely clear. Risk tolerance is effectively the quantification of Council's risk appetite. Risk tolerance which cannot be expressed in financial terms is more difficult to quantify and needs to be closely assessed as risks are identified and analysed. Council's risk tolerances are set out in the likelihood and consequence tables appended to this policy.

6. DOCUMENTATION

6.1 Important ERM processes and activities should be documented throughout Council. Documentation is important because it:

a) Gives integrity to the process and is an important part of good corporate governance;
b) Provides an audit trail and evidence of a structured approach to risk identification and analysis;
c) Provides a record of decisions made which can be used and reviewed in the future;
d) Provides a record of risk profiles for Council to continuously monitor.

6.2 Key documents include the:

a) Enterprise Risk Management Policy;
b) Corporate Risk Register;
c) Risk treatment plans.

6.3 Maintaining key documents

6.3.1 Risk documentation, including risk registers, written/ formal risk assessments, risk/ control audits and self-assessments are to be maintained in TRIM.

6.3.2 These records may be called upon in the management of ongoing treatments, as evidence in incident investigations, in dealing with insurance matters or during other inquiries, and for audit purposes.

6.3.3 ERM records should be reviewed:

a) On the handover of responsibilities between managers;

b) On assumption of responsibility for a project or program;
c) Regularly to match reporting requirements; and
d) Whenever operating parameters are subject to major change

7. ERM ACTIVITIES, REPORTING AND REVIEW

7.1 The ERM framework review

7.1.1 Documentation including policies, processes, risk registers and systems relating to the ERM framework should be subject to periodic review and audit.

7.2 Corporate Risk Register - establishment and review

7.2.1 All managers and directors must establish and periodically review risk registers for their directorates and business units within Council. These risk registers should identify and evaluate key strategic and operational risks that are relevant to their unit in accordance with the process described in part 4 of this policy. The registers should identify and evaluate controls in place to manage those risks and identify any required risk treatment plans. Collectively, these registers comprise the Corporate Risk Register.

7.2.2 Each manager and director should conduct a quarterly review of their business unit/ directorate register in conjunction with Council's quarterly review process. Managers and directors must sign off that their register has been reviewed and that controls are appropriate. Any changes to the register and/ or new or amended risk treatment plans, as a result of this review, are to be reported to the Audit, Risk and Improvement Committee by the HAR. The requirement for a formal quarterly review does not preclude more regular review of risk registers. Regular review of risk registers is encouraged, especially when there are changes in the operating environment and/ or new risks are identified.

7.2.3 The risk register review is an integral part of the annual business planning cycle to ensure that:

a) Risks are identified and assessed in the context of the current objectives of Council, the particular directorate and particular business unit;
b) The status of risks and controls is to be reviewed in conjunction with the review of the performance of each directorate and business unit;
c) If necessary, risk treatment plans are to be included into Council's operational plan;
d) If funding is required to implement risk treatment plans, this requirement is to be included Council's budget.

7.3 Risk treatment plans

7.3.1 Risk owners are responsible for ensuring that actions contained in risk treatment plans (RTPs) are implemented effectively and within agreed timeframes. Action taken must be recorded in TRIM. Risk owners are also responsible for ensuring that actions contained in RTPs are included in their business plans and, where appropriate, in Council's Operational Plan.

7.4 Risk status reports

7.4.1 The HAR is to coordinate the preparation of a quarterly risk status report to be submitted to the Audit, Risk and Improvement Committee. The quarterly risk status report should at least contain the following details:

a) Any ERM initiatives undertaken during the previous quarter;
b) Any major incidents/ claims that have occurred during the previous quarter;
c) The major inherent and residual risks facing Council and the controls in place to manage those risks;
d) Progress in implementing key risk treatment plans;
e) Any issues that may have arisen as a result of the quarterly risk register review by managers and directors.

7.5 Major projects, tenders, procurement and/ or new initiatives

7.5.1 A full risk assessment should be undertaken prior to embarking on any major projects, tenders, procurement activities or other new initiatives. The risk assessment should clearly set out the risks involved and the controls in place (or proposed) to manage those risks. The results of the risk assessment must be included in any report to the Audit, Risk and Improvement Committee or Council, recommending a proposed course of action. The relevant Council manager or director is responsible for ensuring that such an assessment is undertaken.

7.5.2 A formal risk assessment is required if a project or initiative may involve:

a) Significant impact on the community and/ or the environment; or
b) New expenditure or income in excess of $150,000;
c) Significant impact on Council's ability to achieve key objectives; or
d) High potential for fraud, corruption or serious and substantial waste.

7.6 Council's Delivery Program and Annual Report

7.6.1 Council's annual Delivery Program should include a section on ERM, setting out proposed ERM in relation to proposed Council activities for the coming year. In particular, the delivery program should identify key risks that may impact on objectives as well as strategies and controls in place (or proposed) to manage those risks.

7.6.2 Council's Annual Report must include a section on ERM that sets out ERM activities undertaken during the previous year and any relevant ERM issues.

7.7 Training

7.7.1 All risk owners and other key members of Council staff need periodic training in how to implement the ERM process and to be aware of their responsibilities and obligations under this policy. It is recommended that ERM training should be provided to all risk owners and other relevant Council staff every four years.

7.7.2 All new members of Council staff should be informed about Council's commitment to ERM and their responsibilities and obligations, when they commence work with Council.

Further training may be delivered internally or externally or by a combination of the two. Council's Work Health and Safety Coordinator is responsible for coordinating the provision of such training.

7.8 Staff performance management

7.8.1 To emphasise accountability and evaluate ERM performance, ERM should be a key component of regular performance appraisals of directors and managers. ERM responsibilities and accountabilities should also be included in staff position descriptions.

7.9 Other risk assessment activities

7.9.1 To manage specific risks, Council has in place a range of risk assessment processes. (For example, to manage the safety risks specific to particular works and activities, Council has a Work Health and Safety Management System which requires a systematic and detailed assessment of safety hazards and risks.) Specific risks should not be duplicated in the corporate risk register and should not be assessed against the corporate risk matrix, if there are specific matrices and criteria in place for the particular type of risk involved. However, the process for assessing such risks must be consistent with the process described in this policy. This relationship is shown in the following diagram:

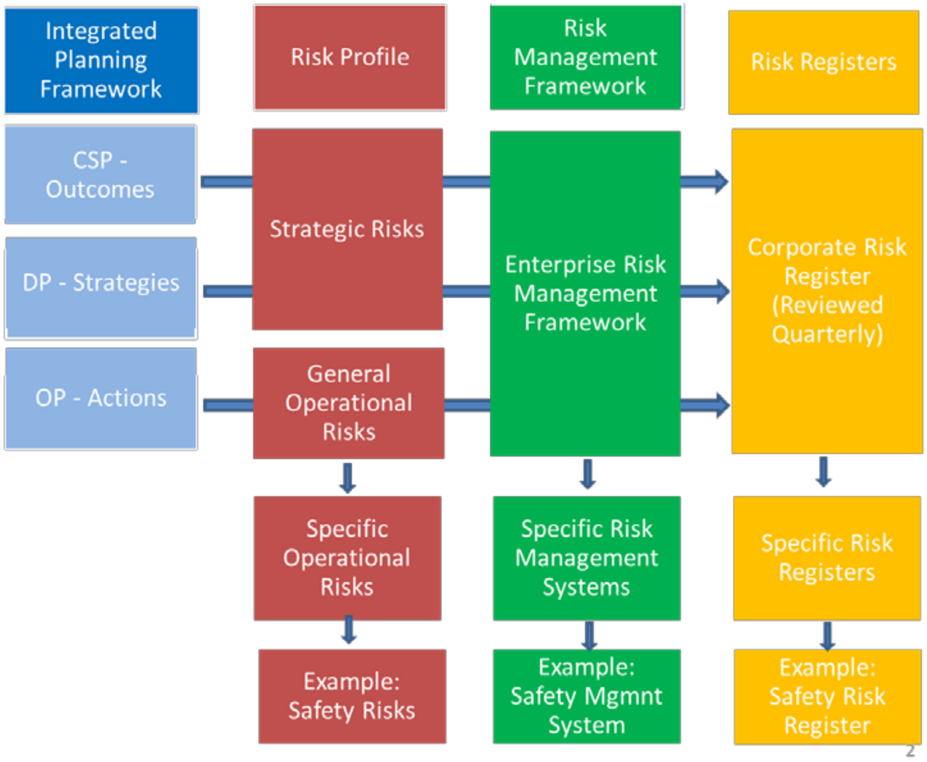
Integrated Planning Framework
Risk Profile
Risk Management Framework
Risk Registers
CSP - Outcomes
DP - Strategies
OP - Actions
Strategic Risks
General Operational Risks
Enterprise Risk Management Framework
Corporate Risk Register (Reviewed Quarterly)
Specific Operational Risks
Specific Risk Management Systems
Specific Risk Registers
Example: Safety Risks
Example: Safety Mgmnt System
Example: Safety Risk Register
2

Figure 1: Relationship between risk registers and corporate objectives

7.10 Annual ERM program

7.10.1 The HAR should submit an annual ERM Program to the CEO for adoption after consultation with the Audit, Risk and Improvement Committee. The ERM program should include the tasks and activities to be undertaken during the year such as insurance renewals, ERM development and ongoing improvement, key risk profiling activities, policy and process development and review, and ERM training. It should also contain performance indicator descriptions and completion dates for each task. The ERM program should consolidate all of the ERM related functions across Council into a single program including work health and safety initiatives and workers compensation claims management as well as business continuity planning. The ERM program should be structured to link to and be aligned with key elements of the operational plan and reporting cycle.

7.11 Communication

7.11.1 Ongoing communication about the importance of ERM and the role of Council staff in managing risk is critical to success of the ERM framework. Accordingly, the HAR should ensure that relevant ERM information is communicated to Council staff on a regular basis. This may be done through a range of mediums, including the Council intranet, newsletters and e-mails.

7.12 Summary of actions, reviews and reports

7.12.1 Appendix A summarises the key actions, reviews and reports required by Council’s ERM process. It assigns responsibility for each activity and the required timing.

8. THE ERM PROCESS

8.1 The ERM process

8.1.1 Council uses the Australian and New Zealand Risk Management Standard AS/NZS ISO 31000:2009 to manage risks. This is a structured and proactive approach applicable across Council to support management of strategic and/ or operational risks. Under this approach, there are five key stages to the ERM process:

a) Communicate and consult - with internal and external stakeholders;
b) Establish context - the boundaries;
c) Risk Assessment - identify, analyse and evaluate risks;
d) Treat Risks – implement and assess controls to address risk; and
e) Monitoring and review – risk reviews and audit.

(Note: Refer to figure 2 below for an illustration of the AS/NZS ISO 31000:2009 ERM approach.)

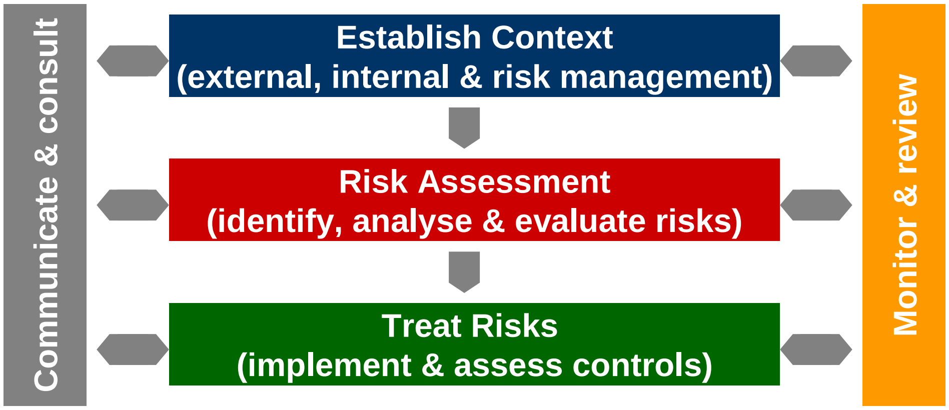
Communicate & consult
Establish Context
(external, internal & risk management)
Risk Assessment
(identify, analyse & evaluate risks)
Treat Risks
(implement & assess controls)
Monitor & review

Figure 2: Council's ERM approach using AS/NZS ISO 31000 ERM Standard

8.2 Establish context

8.2.1 Establishing the context of ERM at Council is the foundation of good ERM and vital to successful implementation of the ERM process.

8.2.2 Context involves setting boundaries around the depth and breadth of ERM efforts to help Council staff to remain focused and align the ERM framework to relevant matters.

8.2.3 Important considerations when determining context include:

a) Objectives: ensuring that the objectives of the particular process, function, project that is the subject of a risk assessment are clearly defined and understood
b) Council's external environment: social, demographics, environmental and economic factors;
c) Council's stakeholders: residents and ratepayers, the Mayor and Councillors, customers, Council staff, the media, service providers and volunteers;
d) Council's internal environment: goals, objectives, culture, risk appetite/ tolerance, Council's organisational structure, systems, processes, resources, key performance indicators and other drivers.
e) Council's appetite for risk: the amount of risk that Council should accept in pursuit of its objectives.

8.3 Risk identification

8.3.1 Risk identification is the process of identifying risks facing Council. This involves thinking through the sources of risks, the potential hazards and opportunities, the possible causes and the potential exposure.

8.3.2 The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

8.3.3 Risk identification occurs within the context of the ERM activity or process. The following categories of risk should typically be considered:

a) Strategic risks; and
b) Operational risks:

1) Financial risks;
2) Reputational risks;
3) Legal and regulatory risks;
4) Business disruption;
5) Human risks (including safety); and
6) Environmental risks

8.3.4 It is important to undertake a systematic and comprehensive identification of all risks, including those not directly under the control of Council, because a risk that is not identified at this stage should not be included in further analysis. The key questions when identifying risks are:

a) What can happen?
b) Where can it happen?
c) When can it happen?
d) Why can it happen?
e) How can it happen?
f) What is the impact? and
g) Who is responsible for managing the risk?

8.3.5 Council may use a number of methods to help identify risks that could materially impact its functions and activities. These include:

a) Brainstorming;
b) Formal risk workshops and consultation with stakeholders;
c) Personal experiences;
d) Expert judgement;
e) Periodic working committee meetings;
f) Periodic reviews of the risk register;
g) Scenario analysis;
h) Business process reviews and work breakdowns;
i) Review of actual incidents and issues identified; and
j) SWOT analysis.

8.3.6 It is also important to consider the potential causes of a risk as it should help to address the risk - the next stage of the ERM process. Some causes of risk could include:

a) Commercial/ legal relationships;
b) Socio-economic factors;
c) Political/ legal influences;

d) Personnel/ human behaviour;
e) Financial/ market activities;
f) Management activities and controls;
g) Technology/ technical issues;
h) The activity itself/ operational issues;
i) Business interruption; and
j) Natural events.

8.4 Risk analysis

8.4.1 Once risks have been identified, they are then analysed. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. At this point, no consideration is given to existing controls. The following risk criteria should be used as a guide when analysing risks:

a) The likelihood of occurrence is the probability of an event occurring. When considering the likelihood of a risk, both the probability and frequency of occurrence must be considered. Council should use the likelihood ratings shown in Appendix B;
b) The consequence assessment is the effect or impact of the risk event. Council should use the consequence ratings shown in Appendix C;
c) Inherent risk is the overall raw risk. It is determined by combining the likelihood and consequence ratings. Ultimately, the level of inherent risk should determine how a risk is treated. The table shown in Appendix D depicts the inherent risk levels that should be used by Council.

8.5 Risk evaluation

8.5.1 Risk evaluation involves comparing the level of risk found during the analysis process against Council's known priorities and requirements.

8.5.2 Any risks accorded too high or too low a significance should be adjusted, and documented accordingly. The output of the risk evaluation is a list of prioritized risks for further action.

8.6 Risk treatment

8.6.1 Risk treatment involves selecting one or more options for modifying risks, and implementing those options. It involves identifying and evaluating existing controls and management systems to determine if further action (risk treatment) is required.

8.6.2 Existing controls are identified and then assessed as to their level of effectiveness. Council should use the control effectiveness ratings shown in Appendix E.

8.7 Residual risk

8.7.1 Residual risk is the level of risk after considering existing controls. It is determined by applying the effectiveness of existing controls to inherent risk. The table in Appendix D - Risk Level Ratings (see above) should also be used to determine the level of residual risk. Ultimately, the level of residual risk should determine how a risk is treated.

8.7.2 Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) Taking or increasing the risk in order to pursue an opportunity;
c) Removing the risk source;
d) Changing the likelihood;
e) Changing the consequences;
f) Sharing the risk with another party or parties (including contracts and risk financing);
g) Retaining the risk by informed decision.

8.7.3 When a residual risk is assessed as medium or above and a decision is made that the risk is not acceptable, a risk treatment plan should be developed to reduce the risk to an acceptable level within an appropriate timeframe.

8.7.4 The information provided in risk treatment plans should include:

a) The reasons for selection of treatment options, including expected benefits to be gained;
b) Those who are accountable for approving the plan and those responsible for implementing the plan;
c) Proposed actions;
d) Timing and schedule.

8.7.5 For the various levels of residual risk, the following escalation process must be followed:

a) High or extreme: Requires immediate risk treatment as the potential risk exposure could be devastating to the Council. The existence of a high or extreme residual risk and any proposed action to further treat such a risk must be reported to the CEO and/ or Audit, Risk and Improvement Committee for consideration as soon as possible. The Audit, Risk and Improvement Committee and/ or the CEO must determine whether the proposed risk treatment, including the time frame for implementation, is acceptable. In some rare cases, the Audit, Risk and Improvement Committee and/ or the CEO may determine to accept a high or extreme residual risk without further treatment, where the cost of treatment exceeds the benefit and the objective being pursued is considered critical. In such cases, the reason for accepting the risk without further treatment must be documented.
b) Medium: May require action at some point in the near future, as it has the potential to be damaging to the Council. Medium risks and any proposed action to further treat such risks must be reported to the CEO, the relevant director and/ or the Audit, Risk and Improvement Committee for consideration as soon as practicable. The CEO, the relevant director and/ or the Audit, Risk and Improvement Committee must determine whether the proposed risk treatment, including the time frame for implementation, is acceptable. Medium risks may be accepted in some circumstances, most likely when

the cost of further treatment exceeds the benefit. In such cases, the reason for accepting the risk without further treatment must be documented.

c) Low: Low risks are generally acceptable and do not require any formal sign off. Low risks should continue to be monitored and re-evaluated on a regular basis. Low risks can generally be treated with routine procedures.

8.8 Monitoring and review

8.8.1 Few risks remain static. Risks should be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk treatment plans should be assessed to ensure changing circumstances do not alter risk priorities. Feedback on the implementation and the effectiveness of this policy should be obtained from the risk reporting process, internal audits and other available information.

8.8.2 Key risk indicators (KRIs) should be developed to monitor risks on an ongoing basis. KRIs are operational in nature and should be determined by the risk owner, once risks and their causes have been identified.

8.9 Communication and consultation

8.9.1 Effective communication and consultation with key stakeholders regarding ERM processes, issues and initiatives is critical to the success of Council’s ERM framework. Internal Audit staff must ensure that relevant stakeholders are informed, consulted and, if necessary, involved in ERM activities that affect them or for which they may be able to contribute. In particular, stakeholders who may be affected by, or may have knowledge regarding, risks must be consulted in relation to the assessment and evaluation of such risks.

8.10 External specialists

Given the size and risk profile of Council, external specialists may be needed from time to time to assist the Council in evaluating and treating risks.

AUTHORISED BY

Council Resolution

EFFECTIVE FROM

28 June 2017

DIRECTORATE/ UNIT RESPONSIBLE

Office of the Chief Executive Officer (Internal Audit)

REVIEW DATE

28 June 2019

VERSIONS

Version	Amended by	Date	Changes made	TRIM Number
1	Adopted by Council	16 December 2014	Not applicable	117975.2014
2	Adopted by Council	28 June 2017	Merging of ERM Strategy and ERM Policy	103446.2017

THIS POLICY HAS DEVELOPED AFTER CONSULTATION WITH

Audit Risk and Improvement Committee
Corporate Services (Governance, Legal Services and Procurement)

REFERENCES

Australian Standard AS/NZS ISO 31000:2009 Risk Management
Liverpool City Council: Audit, Risk and Improvement Committee Charter
Liverpool City Council: Fraud and Corruption Prevention Policy
Liverpool City Council: Internal Audit Charter
Liverpool City Council: Work Health and Safety Policy

Appendix A

Summary of Key ERM Activities

Reference	Action	Description	Responsibility	Timing
4.1	Review ERM Policy	Review the currency and effectiveness of Council's ERM Policy	Council to adopt (with prior review by the HAR and then endorsement by Audit, Risk and Improvement Committee)	Every two years
4.2	Review Corporate Risk Register	Review risks and controls contained in Council's corporate risk register and identify new or emerging risks	All directors and managers (risk owners) to complete review and report as part of the Quarterly Review process	Every quarter in conjunction with Quarterly Review Process
4.3	Include RTPs in Operational Plan	Ensure that actions required by risk treatment plans are included in the Operational Plan	All directors and managers (risk owners) overseen by the HAR	Every year/ quarter in conjunction with Operational Plan development/ review
4.4	Implement RTPs	Implement actions contained in risk treatment plans	All directors and managers (risk owners)	As identified in relevant RTPs
4.5	Risk status report	Identify and review, by exception, any risk issues arising from the quarterly risk register review and the current status of key risks, RTPs, incidents and other relevant issues	Audit, Risk and Improvement Committee (coordinated by the HAR)	Quarterly
4.6	Risk assessments for major projects/ initiatives	Conduct risk assessments required for major new or altered activities, processes or events	Relevant manager/ director (risk owner) The HAR to assist.	Prior to deciding to proceed with new project/ initiative
4.7	Annual Report	Specify ERM activities undertaken during the previous year and any relevant ERM issues	The HAR	Annual

4.8	Operational Plan	Identify key risks that may have an impact on objectives as well as strategies and controls in place (or proposed) to manage those risks.	Managers and directors (risk owners) overseen by the HAR	Annual
4.9	Training	Ensure risk owners and other members of Council staff are aware of ERM process and their obligations	The HAR	Refresher for all directors and managers (risk owners) every four years.
4.10	Staff position descriptions and performance review	Ensure ERM responsibilities are included in position descriptions and employment contracts and that performance of directors and managers is assessed on a regular basis	Manager People and Organisational Development	Annual
4.11	ERM Program	Specify proposed ERM activities and objectives for the next 12 month period	The HAR	Annually in June/ July
4.12	Communication	Ensure members of Council staff are aware of relevant ERM issues and have access to ERM tools.	The HAR	Ongoing

Appendix B

Likelihood Ratings

Rating	Likelihood	Description	Quantification
1	Rare	The event may occur but only in exceptional circumstances. No past event history.	Once every 50 years or more. Less than 10% chance of occurring.
2	Unlikely	The event could occur in some circumstances. No past event history.	Once every 20 years. Between 10% and 30% chance of occurring.
3	Possible	The event may occur sometime. Some past warning signs or previous event history.	Once every 5 years. Between 30% and 70% chance of occurring.
4	Likely	The event will probably occur. Some recurring past event history	Once a year. Between 70% and 90% chance of occurring.
5	Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history.	Several times a year. Greater than 90% chance of occurring.

Appendix C

Consequence Ratings

Impact on objectives		Area	Impact on specific Council operations (to guide assessment)
Severe	Most objectives can no longer be achieved. Complete revision of long term business model required.	Financial	>$2m recurrent reduction in operating budget, one off loss of > $10m
		Environmental	Very serious irreversible damage to environment and/ or multiple sites or ecosystems, prosecution of Council
		Reputation	Sustained negative metropolitan or national media coverage, widespread public outcry and loss of trust in Council, damage to Council reputation that takes many years to repair, investigation resulting in prosecution or dismissal of elected Council
		Legal	Serious breaches of legislation, successful class action against Council, imprisonment or fines for senior management
		Service disruption	Key activities and essential services disrupted for over 14 days
		Human	Major negative impact on Council staff morale, loss of life, major repeated breaches of WHS legislation resulting in prosecution of Council
Major	A number of significant business objectives can no longer be achieved.	Financial	$1m-$2m recurrent reduction in operating budget, one off loss of $3m- $10m
		Environmental	Significant long term impacts on built and natural environment,
		Reputation	Significant adverse media stories at state and local level, strong and ongoing complaints from residents over a long period of time
		Legal	Serious breaches of laws and regulations resulting in fines, major legal actions over an extended period, multiple insurance claims
		Service disruption	Key activities disrupted for between 7 and 14 days
		Human	Major impact on staff morale, breaches of legislation, lost time, injuries requiring major medical treatment
Moderate	Some important business objectives can no longer be achieved.	Financial	$250k-$1m recurrent reduction in operating budget, one off loss of $1m-$3m
		Environmental	Serious medium term effects on built and natural environment from a single incident (such as a one-off pollution spill)
		Reputation	Concerns from broad spectrum of residents, major local media coverage (short duration), opportunistic fraud by a staff member
		Legal	Minor breach of legislation resulting in warnings and, breach notices, one-off claims or legal matters requiring management attention
		Service disruption	Key activities disrupted for between 3 and 7 days
		Human	Minor breach of WHS legislation, short duration of lost time for injuries requiring minor medical treatment
Minor	Some changes in reallocating resources to enable	Financial	$50k-$250k recurrent reduction in operating budget, one-off loss of $250k-$1m
		Environmental	Short term effects on built and natural environment, damage to a single property or parcel of land, breach of policy

	business objectives to be achieved	Reputation	Heightened concerns from a small group of residents, some media concerns
		Legal	One-off claims or legal matters resolved through routine procedures, technical breaches of regulations
		Service disruption	Some Council activities disrupted for up to 3 days
		Human	Some short term impact on Council staff morale, minor injuries or illness from normal activities treated by first aid
Very Low	Little or no impact on business objectives	Financial	<$50k recurrent reduction in operating budget, one off loss of <$250k
		Environmental	Minor effects on built and natural environment, breaches of guidelines, perception of damage
		Reputation	One-off insignificant adverse local media or public complaints
		Legal	Minor claims or investigations that are easily defended or responded to
		Service Disruption	Usual scheduled interruptions, unscheduled interruptions for less than 4 hours
		Human	In-house staff concerns, minor incidents and/ or “near misses”

Appendix D

Risk Rating Matrix

	Consequence				
Likelihood	1 Very Low	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost Certain	Medium	Medium	High	Extreme	Extreme
4 Likely	Low	Medium	Medium	Extreme	Extreme
3 Possible	Low	Low	Medium	High	Extreme
2 Unlikely	Low	Low	Medium	Medium	High
1 Rare	Low	Low	Low	Medium	Medium

Appendix E

Control Effectiveness Ratings

Rating	Effectiveness	Description	Quantification
0	Not Effective	The control does not address risk	0%
1	Slightly Effective	The control is not reliable as it is not well designed, documented and/or communicated.	1-20% effective
2	Somewhat Effective	Control may be reliable but not very effective as control design can be improved.	21-40% effective
3	Reasonably Effective	Control is reliable but not effective as documentation and/or communication could be improved.	41-60% effective
4	Mostly Effective	The control is mostly reliable and effective. Documentation exists but can be better communicated.	61-80% effective
5	Very Effective	Control is reliable and effective. Fully documented process and well communicated.	81-100% effective

Appendix G

ERM Glossary

Adapted from AS/NZS ISO 31000

communication and consultation	continual and repetitive processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** and others regarding the management of **risk stakeholder** person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
consequence	outcome of an **event** affecting objectives
control	measure that is modifying **risk**
establishing the context	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** for the **ERM policy**
ERM	coordinated activities to direct and control an organisation with regard to **risk**
ERM framework	set of components that provide the foundations and organisational arrangements for designing, implementing, **monitoring**, reviewing and continually improving **ERM** throughout the organisation
ERM strategy	scheme within the **ERM framework** specifying the approach, the management components and resources to be applied to the management of **risk**
ERM policy	statement of the overall intentions and direction of an organisation related to **ERM**
ERM process	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, **monitoring** and reviewing **risk**
external context	external environment in which the organisation seeks to achieve its objectives
internal context	internal environment in which the organisation seeks to achieve its objectives
level of risk	magnitude of a **risk**, expressed in terms of the combination of **consequences** and their **likelihood**
likelihood	chance of something happening
monitoring	continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

residual risk	risk remaining after risk treatment
review	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
risk	effect of uncertainty on objectives
risk analysis	process to comprehend the nature of **risk** and to determine the **level of risk**
risk assessment	overall process of risk identification, risk analysis and risk evaluation
risk attitude	organisation's approach to assess and eventually pursue, retain, take or turn away from **risk**
risk aversion	attitude to turn away from **risk**
risk criteria	terms of reference against which the significance of a **risk** is evaluated
risk evaluation	process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable
risk identification	process of finding, recognizing and describing **risks**
risk owner	person or entity with the accountability and authority to manage the **risk**
risk profile	description of any set of **risks**
risk source	element which alone or in combination has the intrinsic potential to give rise to **risk event**
risk treatment	process to modify **risk**