LIVERPOOL PLAINS SHIRE COUNCIL
RISK MANAGEMENT POLICY

Version	Date	Resolution No	Details
1	31 Oct 2018	3080	New Policy

POLICY OBJECTIVE

The purpose of this policy is to implement an organisation approach to Risk Management to minimise Council's exposure to risk while maximising cost effectiveness

RELEVANT LEGISLATION

AS/NZS ISO 31000:2018.

EFFECTIVE DATE AND POLICY REVIEW

The policy shall be reviewed every four years or earlier if required by legislation, Council resolution or recommendation of the General Manager. If the policy is not reviewed within this timeframe, it remains active until such time as it is reviewed or revoked by Council.

This policy comes into effect on 31 October 2018

Signed by General Manager ____________________________________

R S (Ron) van Katywk

Date Approved 31 October 2018

1 INTRODUCTION

1.1 The Risk Management Policy

This document describes the risk management policy and framework (RMP) of Liverpool Plains Shire Council (LPSC). The RMP outlines the risk appetite of the Council, and the systematic method used to identify, analyse, evaluate, treat, monitor and communicate key risks associated with Council responsibilities in order to minimise unexpected losses and maximise opportunities. The RMP is consistent with the requirements of the Local Government Act 1993 and associated regulations. It is also aligned with the Australian Standard AS/NZS ISO 31000:2018 *Risk Management,* and the Internal Audit guidelines issued by the Department of Local Government in October 2008. The RMP takes into account the context of Council responsibilities and objectives as stated in the LPSC Community Strategic Plan and the Management Plan. The RMP also reflects the Enterprise Wide Risk Management Framework (the Framework) of LPSC.

1.2 Council Risk Appetite

Council is periodically updated on the effectiveness of the management of key Council potential risk exposures, through reports from the Audit, Risk and Improvement Committee. The Audit, Risk and Improvement Committee receives a risk report from the General Manager periodically to provide them with relevant information to oversight the effectiveness of the risk management framework and processes, owned by the General Manager.

The risk appetite of Council is reflected by the combination of the severity ratings within the Potential Consequence table and the Likelihood table (section 2.2.3.3) which provides an inherent risk rating. The inherent risk rating is based on the assumption that there are no controls in place to treat the risk. The General Manager, through the Directors, periodically identifies and evaluates the internal and external risks to the achievement of Council objectives and determines the most appropriate means to manage those risks within pre-determined tolerance levels.

The pre-determined tolerance levels are set out through ongoing review of the Risk Profile of Council (section 3.). The risk profile classifies risk as “Critical, high”, “moderate”, or “low.” A risk that is rated above the tolerance level is escalated appropriately and actions are taken to move the risk to an acceptable level.

1.2.1 Determinants of Risk Appetite

The key determinants of risk appetite include:

- Council and Community preferences and expectations
- the income potential from accepting risks relative to income from risk-free activities (the risk/reward trade off)
- capital availability
- culture suitability
- adequacy of risk management skills
- recent track record in managing these risks.

1.3 Council Commitment

The Council is committed to ensuring that risks are adequately and appropriately identified and addressed in a timely way through this RMP. It is the policy of Council to adhere to this RMP at all times.

Council is enhancing its risk management culture through training programs and establishing risk-related performance objectives for individuals.

1.4 Definitions

The following terms are defined for the purposes of this RMS:

Risk An event that may result in potential loss resulting from inadequate or failed internal processes, people, systems or external events.

Key risk A risk that has the potential, if realised, to adversely affect the objectives and strategy of LPSC. If a key risk event occurs, consequences may be financial, reputational, or operational.

Inherent Risk Rating The potential consequence and likelihood of a risk event occurring in an environment without controls.

Residual Risk Rating The potential consequence and likelihood of a risk event occurring after consideration of the effectiveness of treatment/controls in place to mitigate the risk.

1.5 Structure of this Document

Part A of this document sets out the measures and procedures used by the Council to identify, monitor and manage risk.

Part B of this document sets out the relevant key risks identified by the Council and an analysis and evaluation of those risks.

2 PART A

The Council recognises that it is critical to its long-term success and sustainability that it has in place robust and comprehensive Governance and Risk Management Frameworks.

2.1 Council Governance Framework

Council Governance Framework is structured to support effective and efficient decision-making, as well as fostering a culture that is accountable and responsive to the expectations of the community and its regulators.

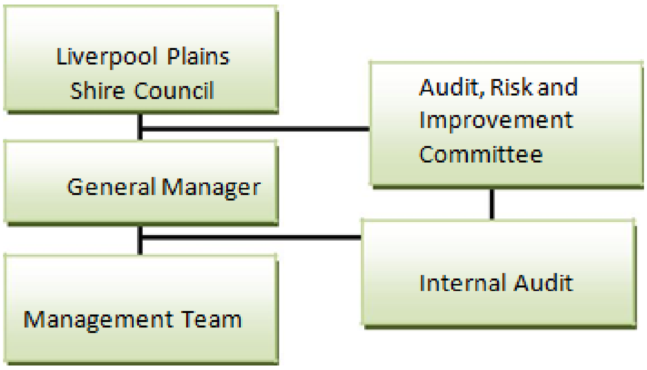
2.1.1 The Council

The Council is responsible for approving and reviewing governance and risk management strategy and tolerances, and monitoring progress, performed through the mechanism of the Audit, Risk and Improvement Committee.

2.1.2 Governance Structure

Council has a number of Committees (and Sub-Committees) that assist the Council in the proper performance and discharge of their responsibilities. The diagram below illustrates the Audit, Risk and Improvement Committee within the organisational structure.

COUNCIL GOVERNANCE STRUCTURE


Liverpool Plains Shire Council
Audit, Risk and Improvement Committee
General Manager
Internal Audit
Management Team

2.2.1 Roles and Responsibilities for Risk Management

Audit, Risk and Improvement Committee

The Audit, Risk and Improvement Committee is responsible for the oversight of the risk management process across Council. The Audit, Risk and Improvement Committee Charter sets out the details of level of oversight and monitoring required by the Committee. The Committee receives periodic reports on the status of the risk management plan from the General Manager. The Committee also receives reports from the Internal Auditor based on the approved Internal Audit Strategy and Plan.

General Manager

The General Manager is responsible for implementing and ensuring ongoing compliance with the risk management policy and process across Council. The General Manager is responsible for ensuring that key risks are identified, evaluated, assessed, monitored and addressed in accordance with the RMP. The General Manager is responsible for ensuring that the risk profile of Council is periodically reviewed, updated and reported to the Audit, Risk and Improvement Committee.

Directors

Directors are responsible for ensuring the compliance of their department with the RMP and the promotion of a positive risk and compliance culture that embraces the philosophy of the RMP. Directors are responsible for identifying, evaluating, assessing, treating and monitoring the key risks that might potentially prevent them from achieving their objectives and their management plan, as well as ensuring that their staff are adequately trained and competent to perform their duties. Directors are required to advise the General Manager of new potential risks and their assessment of the rating of the new risk, in their area of responsibility as they arise. In addition, if an event occurs that may result in a change of risk rating then Directors are also required to discuss this with the General Manager as they arise.

Internal Audit

Internal Audit provides an independent review function to Council. Internal Audit, in accordance with the Internal Audit Strategy approved by the Audit, Risk and Improvement Committee, evaluate, test and report on the design and effectiveness of internal controls that are in place to manage the key risks of Council. An annual risk based Internal Audit Plan is also approved by the Audit, Risk and Improvement Committee.

2.2.3 Risk Management Methodology

The Council utilises a risk management methodology that is aligned with Australian Standard AS/NZS 31000:2018 *Risk Management to* conduct risk assessments. The current risk assessment for Council is summarised in Appendix 1.

2.2.3.1 Establishing the Risk Management Context

The following information/techniques have been utilised in establishing the context for the Council Risk Assessment:

- Council Strategic Plan and Management Plan
- Management Reports
- Council Policies
- Department of Local Government Guidelines
- Better Practice Review Report
- Council Meeting Papers
- Risk Identification Meetings with Directors
- Risk & Control Rating Workshop

2.2.3.2 Risk Identification

The Risk Profile for Council is derived from consultation with senior management. Risks can be identified in any of the following ways:

- Facilitation of a workshop with directors and managers
- Interviews with key staff in each Department
- Quarterly risk questionnaire to all Directors and results follow-up
- Director self assessment
- Reviewing reports issued by Internal Audit
- Reviewing the Incidents Register – the incident register captures all moderate and high incidents that have occurred in Council.

2.2.3.3 Risk Analysis

Inherent Risk Analysis

Inherent risk is defined as the level of risk in the absence of controls. Identified risks are assessed to determine the key risks. Those risks with an Inherent risk rating of medium or above are assessed as key.

Residual Risk Analysis

Once all the inherent material risks have been identified, further risk analysis is undertaken to assess residual risk either in a workshop style meeting or via senior management forums. Effectively, the residual risk analysis is a business self-assessment.

Residual risk is rated in order to effectively assess the level of risk once the control environment is taken into consideration. The determination of residual risk is considered with respect to other monitoring mechanisms such as the Incidents Register, and internal/external audit issues, using the methodology described below.

Assessment of Controls

The controls in place to mitigate risks are assessed on two levels – design effectiveness and operational effectiveness. Design effectiveness will be assessed and rated on the design of the control and its alignment with the risk. Operational effectiveness will be assessed on the results from a monitoring program developed for testing the adequacy and effectiveness of key controls.

The controls are then given an operational effectiveness rating based on the outcome of the monitoring work and any other relevant information such as incidents and internal audit issues. The controls are rated for operational effectiveness using the rating system set out in the table below:

Control Rating	Control Rating Description
Effective	The control framework is appropriate and effective (ie. no evidence of significant risk issues or incidents resulting from the control)
Qualified	Significant control issues have been identified and satisfactory action plans are in place to address the issues within a reasonable timeframe
Requires Improvement	Severe control issues have been identified, and the control environment is inappropriate and/or ineffective - urgent Management attention is required to avoid, reduce or control the risk

Inherent Risk Likelihood Assessment

The inherent risk likelihood (probability) represents the possibility that a given event will occur, in an environment without controls. Likelihood is assessed and rated according to the following categories:

1Rare	<5%
2Unlikely	5 – <30%
3Occasional	30 - <60%
4Likely	60 - <80%
5Almost certain	80 - <100%

This table below is used to rate the inherent risk likelihood for each risk:

Likelihood Table

	Likelihood Level				
	5 Almost Certain	**4 Likely**	**3 Occasional**	**2 Unlikely**	**1 Rare**
Description	- The occurrence of the event(s) necessary for the risk to materialise is almost certain in the foreseeable future. - The expected frequency of the event(s) is more than once every year.	- The occurrence of the event(s) necessary fo the risk to materialise is likely, but not almost certain the foreseeable future. - The expected frequency of the event(s) is once every 1-3 years	- The occurrence of the event(s) necessary for the risk to materialise is possible, but not likely in the foreseeable future. - The expected frequency of the event(s) is once every 3-5 years.	- The occurrence of the event(s) necessary for the risk to materialise is unlikely, but not almost impossible in the foreseeable future. - The expected frequency of the event(s) is once every 5-10 years.	- The occurrence of the event(s) necessary for the risk to materialise is rare in the foreseeable future. - The expected frequency of the event(s) is less than once every 10 years.

Inherent Risk Consequence Assessment

The inherent risk consequence (impact) of risk represents the plausible worst case scenario consequence if the risk event occurred, in an environment of no controls. It is categorised according to following levels of impact on the achievement of Council strategy and objectives:

1	Insignificant
2	Minor
3	Medium
4	Major
5	Catastrophic

The categories to consider when rating inherent risk consequence are:

a Financial
b Reputation
c Operational

This table below is used to rate the inherent risk consequence for each risk:

Consequence Table

Consequence Types		Severity Level			
	5. Catastrophic	4. Major	3. Medium	2. Minor	1. Insignificant
$	▪ Direct loss or opportunity cost with > A$10M impact	▪ Direct loss or opportunity cost with A$2-10M impact	▪ Direct loss or opportunity cost with A$250K-2M impact	▪ Direct loss or opportunity cost with A$50K-250K impact	▪ Direct loss or opportunity cost with < A$50K impact
Operations	▪ Key project failure ▪ Information systems or security failure causing permanent loss of critical business information ▪ Event resulting in death ▪ A major environmental incident	▪ Key project delays / under-delivery resulting in material impact on planned project outcomes ▪ Information systems failure causing temporary loss of information delays ▪ Decreasing population ▪ Skilled staff turnover of more than 5 p/a Event resulting in multiple serious injuries	▪ Key project delays but no material impact on quality outcome ▪ Breach of information security without loss of information ▪ Skilled staff turnover between 3 and 5 ▪ Event resulting in serious injury ▪ An isolated environmental incident	▪ Non-key project delays or under-delivery of planned outcomes ▪ Evidence of attempted breach of information security ▪ Skilled staff turnover between 2 and 3	▪ Information system unavailable for 1 day or less
Reputation	▪ Significant adverse national media coverage ▪ Regulatory sanctions	▪ ICAC investigation ▪ Significant state media coverage ▪ Adverse national media coverage	▪ Adverse regional media coverage ▪ Potential breach of regulations ▪ Community protests / strikes	▪ Local Government sector knowledge of incident, but no media attention ▪ Some impact on community support	▪ No reputation damage – internal knowledge only ▪ Minimal or no impact on community support

Inherent Risk Rating

The potential consequence and likelihood of each risk identified is combined to determine the Inherent Risk Rating. Inherent Risk Ratings are critical, as they are the basis for identifying the most critical risks that need to be treated by management. Internal Audit develops the Internal Audit Strategy by reference to the risks with the highest inherent risk rating.

The table below, which is consistent with the Australian Standard AS/NZS ISO 31000:2018 Risk Management, is used to determine the Inherent Risk rating for each risk. The information from the risk assessment process is fed into risk & control profiles which form the basis for a risk map for Council.

Job Hazard Assessment

Consequence

Rare
(once in five to ten years)

Likelihood

Almost Certain

(once per day to one week)

Likely

(once per week to one month)

Occasional

(once per month to one year)

Unlikely
(once in one to five years)

	Insignificant	**Minor**	**Medium**	**Major**	**Catastrophic**
A	**M7**	**H9**	**H6**	**C3**	**C1**
B	**M8**	**M5**	**H7**	**H4**	**C2**
C	**L3**	**M6**	**H8**	**H5**	**H1**
D	**L4**	**L1**	**M3**	**M1**	**H2**
E	**L5**	**L2**	**M4**	**M2**	**H3**

First Aid	Medical	LTI	Disability	Fatality	**Injury**
< $50K	$ 50K - $250K	$ 250K - $2M	$ 2M - $ 10M	> $ 10M	**Business Impact**
Minor Non-Conformance	Minor Impact	Medium Impact	Major Impact	Catastrophic	**Environment**

2.2.3.4 Risk Evaluation and Treatment

All risks with an inherent rating of Moderate or above are considered key risks and risk treatment is determined and implemented by the manager who owns the risk, as nominated by the General Manager.

Risk treatment involves identifying the range of options for treating the risk and selecting the most suitable to ensure that the residual risk is within limits acceptable to Council. This may result in the Business Unit:

- accepting the risk;
- transferring the risk to a third party (e.g. outsourcing, insurance);
- avoiding the risk altogether by changing the nature of the business (e.g. withdrawing products, avoiding jurisdictions); or
- mitigating the risk.

Generally the risks affecting Council are treated through a treatment strategy of mitigation through implementation of internal controls, or through transfer of risk through insurance.

2.2.3.5 Internal Controls

Internal Controls are a method of mitigating risks. Internal controls can either be preventative, detective, or recovery in nature.

Preventative controls are designed to stop a potential risk event from occurring. An example of a preventative control is dual signatures being required for disbursements over a set dollar value. Another example is automated data validation controls built into data input fields for data processing. Physical security of premises is also a preventative control.

Detective controls are designed to identify problems, mistakes or processing errors so that they can be rectified in a timely manner. Management review of reports or transactions or reconciliations if performed in a timely manner are considered detective controls.

Recovery controls are used to reduce the impact of a risk event that has already occurred. For example if there is an emergency situation that prevents access to Council buildings (perhaps fire or flood), then a recovery control would be the enactment of the Council business continuity plan.

Internal controls are assessed for every risk identified in order to establish the level of residual risk that the Council would be impacted by should the potential risk event occur. The result of combining the Inherent Risk Rating with the Control rating is a Residual Risk Rating. Internal Controls are assessed as either **Effective**, **Qualified** or **Requires Improvement**.

Effective controls are designed and implemented appropriately and reduce the likelihood and in some cases also the consequence of Inherent risks. Therefore if controls are assessed as Effective, there is no need to build additional controls or invest in enhancing controls for the risk. If projects or enhancements are underway and not yet implemented, then controls should not be assessed as Effective. Also, if controls are effective, then this means that the residual risk rating is within the risk tolerance of Council.

A **Qualified** control assessment means that the controls are either not designed well or not working properly to mitigate the potential risk consequences to an acceptable level of residual risk. Qualified controls mean that either a new control needs to be designed and implemented or an existing control needs to be improved before the residual risk will be considered tolerable.

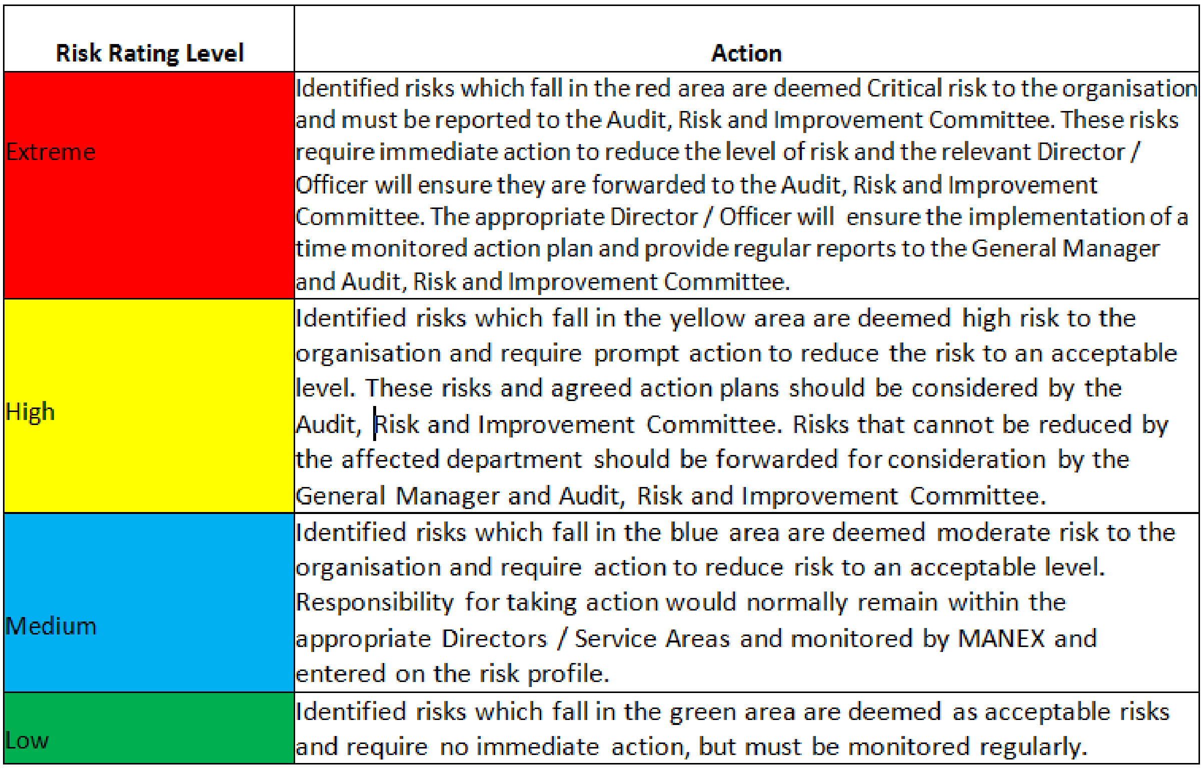
Control assessments of **Requires Improvement** mean that either there are no controls in place because it is a newly identified risk or that existing controls have broken down or are completely inadequate to effectively mitigate the inherent risk. In this case, the Inherent Risk Rating is also the Residual Risk rating and it is critical for management to focus immediately on improving controls for the risk in question.

2.2.3.6 Residual Risk Assessments

Once the Inherent Risk Rating and the Control Assessment has been completed, a residual risk rating is determined. In many cases, the introduction of a detective control will reduce the likelihood of a risk occurring rather than the potential consequence. The introduction of a preventative control can reduce both the consequence and likelihood of an inherent risk.

Management will then determine what (if any) further action is required to reduce, monitor or control the level of residual risk to an acceptable level. Where a residual risk is rated outside the risk appetite (risk tolerance) of the Council, an action is specified in the risk and control profile to ensure appropriate management action. This is an iterative process which continues until the level of residual risk is acceptable to Council. The below table can be used as a guide to the action that may be required.

Action Guidance



Risk Rating Level	Action
🟥 Extreme	Identified risks which fall in the red area are deemed Critical risk to the organisation and must be reported to the Audit, Risk and Improvement Committee. These risks require immediate action to reduce the level of risk and the relevant Director / Officer will ensure they are forwarded to the Audit, Risk and Improvement Committee. The appropriate Director / Officer will ensure the implementation of a time monitored action plan and provide regular reports to the General Manager and Audit, Risk and Improvement Committee.
🟨 High	Identified risks which fall in the yellow area are deemed high risk to the organisation and require prompt action to reduce the risk to an acceptable level. These risks and agreed action plans should be considered by the Audit, Risk and Improvement Committee. Risks that cannot be reduced by the affected department should be forwarded for consideration by the General Manager and Audit, Risk and Improvement Committee.
🟦 Medium	Identified risks which fall in the blue area are deemed moderate risk to the organisation and require action to reduce risk to an acceptable level. Responsibility for taking action would normally remain within the appropriate Directors / Service Areas and monitored by MANEX and entered on the risk profile.
🟩 Low	Identified risks which fall in the green area are deemed as acceptable risks and require no immediate action, but must be monitored regularly.

Communication and Consultation about Risk Management

Internal Reporting

The main forum for reporting of risk management issues is the MANEX. The MANEX is a meeting of the General Manager and the Directors, whose responsibilities are to manage risk and compliance within their departments.

The Director of each department is required to provide a quarterly risk report to the General Manager on key risk issues in their Department. The report will include an update of the key risks that are being owned by the Director. The update will set out changes to risk assessments and also progress on control improvement plans owned by the Director. Where due dates or costs are revised, an explanation of why this has occurred is also required.

2.3 Reviewing and Updating the RMP

The RMP will be reviewed every second year. The purpose of the review is to ensure compliance with the law, efficacy, and ensuring the RMP currently reflects Council strategy and objectives. The General Manager will ensure the Policy is reviewed every second year.

2.4 Audits

Internal Audit provides an independent internal audit function to Council. It develops an annual risk based audit plan and then evaluates, tests and reports on the adequacy and effectiveness of the control environment to manage operational risks.

Appendix 1 Inherent Risk Profile

Table 1. Inherent Risks Identified (numbered for reference purposes only)

	Risk Description	Inherent Risk	Controls	Residual Risk	Review Period	Risk Owner
1	Loss of Water supply / Failure of Water Supply Project	Critical			Quarterly	DES
2	Resident and business dissatisfaction	High				GM
3	Inappropriate focus on commercial ventures – Tr@ceR	High				GM
4	Spread of Noxious/Environmental Weeds	Critical				DEEDS
5	Poor handling of asbestos in Council buildings	High				DEEDS
6	Failure to maintain support from Councillors / Community	High				GM
7	A reactive risk culture across Council	Critical				GM
8	Breach of regulatory and legislative obligations	Critical				GM
9	Inadequate management reporting (financial and non financial)	Critical				CFO
10	Fraudulent misappropriation of council monies	Critical				CFO
11	Failure to deliver successful project outcomes	Critical				GM/CFO
12	Failure of the Cinema Upgrade Project	High				DEEDS
13	Failure of the Dam Recreation Project	Moderate			Yearly	DES
14	Negligence in Childcare Centre	Critical				DEEDS
15	Corruption within the Development Approval / Section 94 Process	High				DEEDS
16	Deterioration of road infrastructure	Critical				DES
17	Breach of Dam Safety Regulations	Critical				DES
18	Breakdown of Water and Sewerage infrastructure	Critical				DES
19	Water Contamination	Critical				DES
20	Inability to effectively deal with community emergencies	Critical				DEEDS
21	Interruption to Council operations	Critical				CFO

	Risk Description	Inherent Risk	Controls	Residual Risk	Review Period	Risk Owner
22	Breach of regulation relating to Quarries	Critical				DES
23	Failure of Drainage Systems	Critical				DES
24	Inadequate reserves to meet unplanned costs	Critical				CFO
25	Payroll errors	High				CFO
26	Poor records management	High				CFO
27	Poor contract management	High				GM
28	Poor town planning decisions	High				DEEDS
29	Poor condition of Council owned buildings	Critical				DEEDS
30	Breach of Council Policy	High				GM
31	Inappropriate selection of service providers	Critical				GM
32	Loss of specialist industry expertise and corporate knowledge	Critical				GM
33	Inappropriate behaviour of Councillors	High				GM
34	Inappropriate behaviour by Volunteers (eg. Home Support)	High				DEEDS
35	Injury to lone workers	Critical				GM
36	Lack of design capability within Council	High				DES
37	Lack of understanding of role responsibilities	Critical				DES
38	Poor customer service	High				DEEDS
39	Outdated IT Infrastructure	High				DEEDS

Key:

GM	General Manager
CFO	Chief Financial Officer
DES	Director Engineering Services
DEEDS	Director Environmental and Economic Development Services