City of MANDURAH

MINUTES OF AUDIT AND RISK COMMITTEE MEETING

HELD ON

TUESDAY 16 JUNE 2020
5.30 pm

IN COUNCIL CHAMBERS, 83 MANDURAH TERRACE MANDURAH

PRESENT:

COUNCILLOR	P JACKSON [CHAIRMAN]	NORTH WARD
MAYOR	R WILLIAMS	
COUNCILLOR	J GREEN	COASTAL WARD
COUNCILLOR	A ZILANI	NORTH WARD
COUNCILLOR	P ROGERS	TOWN WARD
MR	W TICEHURST	INDEPENDENT MEMBER

ELECTED MEMBERS OBSERVING:

COUNCILLOR	C KNIGHT

OFFICERS

MR	G DAVIES	ACTING CHIEF EXECUTIVE OFFICER
MRS	C MIHOVILOVICH	DIRECTOR CORPORATE SERVICES
MR	A CLAYDON	DIRECTOR WORKS AND SERVICES
MRS	T JONES	MANAGER GOVERNANCE SERVICES
MRS	L SLAYFORD	MINUTE OFFICER

OPENING OF MEETING [AGENDA ITEM 1]

The Chairman declared the meeting open at 5.31pm.

APOLOGIES [AGENDA ITEM 2]

Leave of Absence	Apologies
Councillor Schumacher (Non-Committee)	

IMPORTANT NOTE [AGENDA ITEM 3]

The purpose of this Committee Meeting is to discuss and make recommendations to Council about items appearing on the agenda and other matters for which the Committee is responsible. The Committee has no power to make any decisions which are binding on the Council or the City of Mandurah unless specific delegation of authority has been granted by Council.

No person should rely on or act on the basis of any advice or information provided by a Member or Officer, or on the content of any discussion occurring, during the course of the meeting. The City of Mandurah expressly disclaims liability for any loss or damage suffered by any person as a result of relying on or acting on the basis of any advice or information provided by a Member or Officer, or the content of any discussion occurring, during the course of the Committee meeting.

RESPONSE TO PREVIOUS QUESTIONS TAKEN ON NOTICE [AGENDA ITEM 4]

Nil.

PUBLIC QUESTION TIME [AGENDA ITEM 5]

The Committee Chairperson advised of processes, information and advertising undertaken to permit the electronic submission of questions by members of the public. No public questions were submitted for the meeting.

PRESENTATIONS [AGENDA ITEM 6]

Nil.

DEPUTATIONS [AGENDA ITEM 7]

The Chairperson advised of processes, information and advertising undertaken to permit the electronic submission of deputations by members of the public. No deputations were received for the meeting.

CONFIRMATION OF MINUTES [AGENDA ITEM 8]

AR.1/6/20 CONFIRMATION OF MINUTES TUESDAY 19 MAY 2020

MOTION
Moved: Councillor Peter Rogers
Seconded: Councillor A Zilani

That the Minutes of the Audit and Risk Committee meeting of Tuesday 19 May 2020 be confirmed.

CARRIED: 6/0

DECLARATIONS OF INTERESTS [AGENDA ITEM 9]

Nil.

QUESTIONS FROM COMMITTEE MEMBERS [AGENDA ITEM 10]

Questions of Which Due Notice Has Been Given

Nil.

Questions of Which Notice Has Not Been Given

Nil.

BUSINESS LEFT OVER FROM PREVIOUS MEETING [AGENDA ITEM 11]

Nil.

REPORTS FROM OFFICERS [AGENDA ITEM 12]

AR.2/6/20 OFFICE OF THE AUDITOR GENERAL: INFORMATION SYSTEMS AUDIT (REPORT 1)

<u>Summary</u>

The Auditor General has issued a report assessing the general information technology (IT) controls at all State Government entities. Each entity was assessed over six categories; information security, business continuity, management of IT risks, IT operations, change control, and physical security.

A comparison between the report's findings and the City's IT structure and organisation has been undertaken.

Council is requested to note the comparison of the status of the City's information systems controls with the findings of the audit on State Government entities.

Comment

Comments regarding the City's position compared to the control weaknesses are included in Confidential Attachment 1.1.

In addition, the following points are noted:

- Although it is possible to provide information regarding the City's controls it is not possible to conclude what the City's actual score would be, as the OAG report does not provide information regarding the various assessment criteria necessary to allocate a score. Despite that, the comparison is a useful exercise, and is largely favourable with improvements required in risk management and disaster recovery testing.

- Many State Government entities have vastly different and larger systems than the City. Some, such as Health and Education, manage a significant volume of confidential data. While that would not take away from the City's need to achieve at least the basic acceptable score if examined, it does mean that, in some cases, the requirements placed on a government entity may be different or unachievable in the local government environment.

  An example of this can be seen in the comments relating to service level agreements with IT vendors. In the case of the State Government, some services are either outsourced or the vendor maintains significant infrastructure on their behalf. This does not translate directly to the much smaller operation at the City.

- State Government entities and the City share a common highly significant risk; the threat posed by a cyber-attack. It is not feasible for the City to have IT staff dedicated to security issues as is the case in larger entities. Despite this, the IT team has undertaken a continuous education process to ensure that the City's defences are as robust as possible.

Officer Recommendation

That Council note the comparison of the status of the City's general computer controls with the findings of the Auditor General's report on State Government entities as detailed in Confidential Attachment 1.1.

Committee Recommendation

MOTION
Moved: Councillor Peter Rogers
Seconded: Councillor A Zilani

That Council note the comparison of the status of the City's general computer controls with the findings of the Auditor General's report on State Government entities as detailed in Confidential Attachment 1.1.

CARRIED: 6/0

AR.3/6/20 RISK MANAGEMENT POLICY AND RISK MANAGEMENT FRAMEWORK (REPORT 2)

Summary

The City of Mandurah has significant moral, financial and legal responsibilities to exercise effective and efficient governance of services and infrastructure to the community and environment. Effective risk management is essential to the City's success in serving the community, delivering on its objectives and establishing a prosperous future for the City.

Governance Services has recently undertaken a review of the City's Risk Management System in response to the need for an updated corporate-wide Risk Management Framework. As a part of the Risk Management System review, the Risk Management Council Policy POL-RKM 01 and City's Risk Management Framework RMK-02 were reviewed to ensure consistency with the Australian ISO 31000:2018 *Risk Management Guidelines*.

Following consultation, the Audit and Risk Committee is requested to recommend to Council to adopt the amendments to the POL-RKM 01 Risk Management Policy (refer Attachment 2.1) and the Risk Management Framework RKM 02 (refer Attachment 2.2).

Officer Recommendation

That Council:

1. Adopt the proposed amendments to POL-RKM 01 Risk Management Policy as per Attachment 2.1*;*

2. Note the updated RKM-02 Risk Management Framework.

Committee Recommendation

MOTION
Moved: Mr W Ticehurst
Seconded: Councilor Peter Rogers

That Council:

1. **Adopt the proposed amendments to POL-RKM 01 Risk Management Policy as per Attachment 2.1*;***

2. **Note the updated RKM-02 Risk Management Framework.**

CARRIED: 6/0

LATE AND URGENT BUSINESS ITEMS [AGENDA ITEM 13]

Nil.

CLOSE OF MEETING [AGENDA ITEM 14]

There being no further business, the Chairman declared the meeting closed at 5.57pm.

CONFIRMED: ……………………………………………………………….[CHAIRMAN]

Attachments to Audit and Risk Committee Minutes:

Minute	**Item**	**Page**
AR.3/6/20	Risk Management Policy and Risk Management Framework Attachment 2.1	1 - 5
AR.3/6/20	Risk Management Policy and Risk Management Framework Attachment 2.2	6 - 45

Confidential Attachments to Audit and Risk Committee Minutes:

Minute	**Item**	**Page**
AR.2/6/20	Office of The Auditor General: Information Systems Audit Confidential Attachment 1.1	1 - 6

RISK MANAGEMENT

COUNCIL POLICY

POL-RKM 01

Introduction:

As a public authority, the City of Mandurah (the City) is exposed to a broad range of risks which, if not managed, could adversely impact on its ability to achieve the strategic community objectives.

Therefore, the City will implement a risk management system encompassing a Risk Management Framework, this Policy and Risk Management Procedures to identify and address, where practicable, areas of risk within the City. The system adopted will be consistent with *Australian and New Zealand Standard ISO 31000:2018 Risk Management Guidelines* (the Standard).

The intent of this policy is to create an environment where Council, management and staff accept direct responsibility for risk management, through development, implementation and maintaining of effective risk management practices. Risk management is the responsibility of everyone and will be treated as an integral part of the City's culture, policies, protocols and processes.

Objective:

The objectives of the risk management and this policy are:

- ***Protection:*** to safeguard the City's assets - people, financial sustainability, environment, property, reputation and information;
- ***Improved quality:*** to use risk management principles as a tool for improving the reliability, effectiveness and efficiency of services and infrastructure to a consistently high standard;
- ***Increase success:*** strengthen financial and non-financial outcomes by using risk assessments to make better informed decisions and clearly articulate what is achievable;
- ***Minimise adverse impacts:*** to undertake good and proper management of risks in order to prevent loss, damage and minimise harm from the City's services and infrastructure on the community, visitors and the environment; and
- ***Opportunity and innovation:*** to capitalise on opportunities identified, foster creativity and facilitate innovation for future success within a sound environment.

Statement:

1. APPLICABILITY

This policy applies to all risk management activities undertaken by City officers, volunteers, appointed representatives and where applicable, contractors.

2. POLICY REQUIREMENTS

2.1 The City will manage risk in accordance with the Standard, and will, at all levels of the organisation, ensure the following is achieved:

- Design and implement a Risk Management Framework that is consistent with the Standard to provide a common structure for all risk management activities across the City;

- Identify, assess and prioritise the strategic risks for each objective stated in the *City of Mandurah Strategic Community Plan 2020-2040* and ensure risk treatments are implemented progressively based on the level of risk and the effectiveness of the current controls;
- Manage all identified risks and undertake regular review of all identified risks;
- Integrate risk management processes into existing business planning cycles and operational processes across all levels of the organisation;
- Act in accordance with relevant legislation and consider political, social, natural and economic environments when managing risk;
- Create and actively promote a culture of risk awareness across the City through implementation, expectation and equipping staff with risk management tools for individual and organisational development; and
- Ensure resources and operational capabilities are identified and allocated to all aspects of the City's Risk Management Framework.

2.2 All levels of the City shall incorporate the following principles of Risk Management. These principles are the City's commitment to create, value and foster effective and efficient risk management.

The City's risk management approach will:

A. be ***integrated*** into all management planning and operational processes undertaken or overseen by The City;

B. be a ***structured and comprehensive*** approach that is applied to ensure risk management processes are systematic and timely;

C. be ***customised*** to fit seamlessly within The City's diverse strategic, operational and project-based activities and in proportion to the external and internal context in which the City operates;

D. be ***inclusive*** of internal and external stakeholder's knowledge, views and perceptions for transparency and better-informed decision-making;

E. be ***dynamic***, ***current*** and ***responsive*** to anticipate and manage change in a meaningful and timely manner;

F. be based on the ***best available information*** considering historical, current and future expectations as would be reasonably foreseeable;

G. be the ***responsibility of all***, from Council to the CEO to every employee, forming an essential element in the City's 'One Team' culture; and

H. be ***continually improved.***

2.3 The City will use the following elements of the Standard as the model for implementing and managing the risk management process within Council's business operations.

- **General**
  The City will ensure the risk management process becomes an integral part of management, embedded in the culture and practices, and tailored to its business processes.

- **Communication and consultation**
  The City will communicate and consult with external and internal stakeholders during all stages of the risk management process, and will address issues relating to the risk - its causes, its consequences (if known) and the measures being taken to treat it. This process will ensure accountability on the part of those implementing the risk management process.

- **Establish the scope, context and criteria**

  By establishing the context, the City will articulate its risk objectives, consider the external and internal parameters, set the scope and criteria for the risk management process. This will be undertaken in full consideration of the need to justify the resources required to be used in carrying out risk management.

- **Risk identification**

  The City will identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that may create, enhance, prevent, degrade, accelerate or delay the achievement of the City's objectives.

- **Risk analysis**

  The City will identify causes and sources of risk, the positive and negative consequences, and the likelihood of those consequences occurring. Existing controls, their effectiveness and efficiency, will also be considered. The analysis will identify the inherent risk level and residual risk level once controls and treatments have been applied.

- **Risk evaluation**

  The City will compare the level of risk with the established context and criteria for the risk. Risk controls and treatment will then be considered. Such decisions will take into account the wider context including the risk tolerance thresholds of internal and external stakeholders that may be impacted by the risk. Decisions will be made in accordance with any legal requirements and obligations the City may have.

- **Risk treatment**

  The City will select the most appropriate and viable risk treatment option taking into consideration a number of factors including, the costs, expected benefit, legal obligations, economic viability, environment, social responsibilities and economic factors.

  Risk treatments will maintain the City's risk exposure within Council's risk appetite thresholds. Any risks that exceed the residual risk level acceptable threshold will be reported to the CEO and Council for input and sign-off.

RISK MANAGEMENT

- **Monitoring and review**

  The City will implement and integrate a 'monitor and review' process to report on achievements of the risk management objectives.

  Treatment and action plans will also be monitored to ensure continual improvement of the City's performance. Monitoring and review will take place at all stages of the process and in compliance with legislative requirements.

- **Recording and reporting**

  The City will ensure all risk management activities are accurately recorded and traceable. Results of the monitoring and review processes will be reported as appropriate through external and internal avenues including, but not limited to, quarterly reports to Audit and Risk and an annual report to Council. Reports will be used to assess and review the effectiveness of the risk management framework and identify specific areas of need.

- **Responsibility/Accountability**

  The Chief Executive Officer is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Framework and Risk Management Procedure.

  Risk management is everyone's responsibility:

  - All employees are accountable for managing risk within their area of responsibility in accordance with the Risk Management Framework and Procedures.

  - Audit and Risk Committee, in accordance with the Terms of Reference, is to monitor and receive reports concerning the development and implementation of the Risk Management Framework and support Council in fulfilling its governance and risk management oversight responsibilities.

  - Executive Leadership and Management Team will be required to create an environment where managing risk is accepted as the personal responsibility of each member of the organisation, and integrated with planning and operational processes.

  - Each Business Area will be accountable for the management of risks within their area of responsibility in ways that is consistent with the Risk Management Framework and Procedures.

Responsible Directorate:	Corporate Services
Reviewer:	Director Corporate Services
Creation date:	Minute AR.6/6/07, 26 June 2007

RISK MANAGEMENT

Amendments:	Minute G.15/9/09, 15 September 2009 Minute G.43/12/09, 15 December 2009 Minute G.35/2/15, 24 February 2015 Minute G.12/7/19, 23 July 2019
Related Documentation and/or Legislation:	*Local Government Act 1995* *Local Government (Audit) Regulations 1996* *Occupational Safety and Health Act 1984* *Occupational Safety and Health Regulations 1996* *Health (Miscellaneous Provisions) Act 1911* *Health (Public Buildings) Regulations 1992* AS ISO 31000:2018 – *Risk Management – Guidelines*. The City of Mandurah Risk Management Framework 2020 Audit and Risk Committee Terms of Reference

Report 02 Risk Management Policy and Framework Att 2

RESPONSIBLE DIRECTORATE: CORPORATE SERVICES
AUTHOR: GOVERNANCE SERVICES TEAM
VERSION 1.0
JUNE 2020

Table of contents

1. Introduction

The City of Mandurah (the City) has significant moral, financial and legal responsibilities to exercise appropriate, effective and efficient governance of services and infrastructure to the community and environment. Effective risk management is essential to the City's success in serving the community, delivering on its objectives and establishing a prosperous future for the City.

The Risk Management Framework (RM Framework) is the system that provides a standardised basis for all risk management activities undertaken by the City. It unites Council's Risk Management Policy POL-RKM 01 (RM Policy) with the City's Risk Management Procedure (RM Procedure), creating a considered and consistent approach to risk management activities at the City. The components of this document are developed in accordance with the Australian Standard *AS ISO 31000:2018 Risk Management Guidelines*.

The RM Framework gives effect to a 'risk aware' culture. Ultimately, the RM Framework is the foundation that supports the City in effectively and efficiently managing risks in pursuit of the City's objectives and community vision.

The RM Framework will be continuously reviewed by the Chief Executive Officer (CEO) and presented to Council (through the Audit and Risk Committee) for noting every two years.

2. Objective

The objective of this document is to create an effective framework that seamlessly integrates risk management across all levels of the organisation. The RM Framework aims to support the following:

- Ensures risk is a key component in the development of the City's Integrated Planning and Reporting Requirements, including 10-year Strategic Community Plan, Corporate Business Plan and a Long-Term Financial Plan;
- Promotes and improves the understanding of risk management across all levels of the City through the implementation of the City's RM Procedures and guidelines;
- Provides a balanced, documented, structured and systematic process with the size and complexity of the City along with existing time, resource and workload pressures;
- Supports strong corporate governance, compliance with relevant legislation, regulation and policies and informed decision-making processes; and
- Provides clear identification of the roles and responsibilities of the risk management functions.

3. Legislative Context

The risk management system is vital to the City's performance of good governance and legislative compliance. Risk management affects all areas of the organisation and is imposed upon the City by several legislative bodies.

3.1 Local Government Act 1995 expects the City to have a risk management system

The *Local Government Act 1995* (*LGA*) requires local governments to provide for the good government of persons in its district.[1] *LGA* s3.18 qualifies 'good government' with the

[1] *Local Government Act 1995* s3.1

expectation that local governments will manage their services and facilities ***efficiently*** and ***effectively***.

In order to provide efficient and effective management the Western Australian State Government expects local governments to implement a corporate wide risk management system. The State Treasurer has instructed that '*risk management is essential to the optimal operation of the public sector*'.[2]

3.2 Occupational Safety and Health Act 1984 imposes a duty of care on The City to manage risk

The *Occupational Safety and Health Act 1984* (*OSH Act*) s19 imposes a duty on the City to provide a workplace that does not expose its employees to hazards. More specifically, the *Occupational Safety and Health Regulations 1996* requires The City to identify, reduce and manage risks in the workplace.

3.3 Health (Miscellaneous Provisions) Act 1911 requires the City's public buildings to have a risk management plan

The *Health (Miscellaneous Provisions) Act 1911* requires the City to ensure the safety and health of persons in its public buildings. *Health (Public Buildings) Regulations 1992* require risk management plans to be undertaken and implemented during public building approval, occupation and in cases of emergency.[3]

3.4 Emergency Management Act 2005 requires that the City implement emergency risk management strategies

Emergency Management Act 2005 ('*EMA*') s36 stipulates that a local government is to ensure local emergency management arrangements are prepared and maintained in accordance with State Emergency Management Committee risk management strategies. In accordance with emergency risk management obligations the City is to effectively manage Emergency Management and Evacuation Plans, Local Recovery Plans and Business Continuity Plans.

3.5 The City's risk management system is subject to legislated reviews and audits:

The City's implementation and day-to-day operations of its risk management Policy, Framework and Procedures are reviewed in accordance with the following legislation:

- *Local Government (Audit) Regulations 1996* ('*LGA Audit*') s17(a) requires the CEO to review the appropriateness and effectiveness of The City's risk management system;
- *LGA Audit* s10(2) requires a Local Government Auditor to report on the operations of The City; and
- *Auditor General Act 2006* s18 authorises the Auditor General at any time to investigate and examine the compliance, effectiveness and efficiency of The City's functions and report to both Houses of Parliament.

[2] Department of Treasury (2007) *Treasurer's Instructions 825 Risk Management and Security*, Western Australia.
[3] *Health (Public Buildings) Regulations 1992* s4, s26 and s26A

4. Australian Standard on Risk Management – AS ISO 31000:2018

In accordance with Government recommendations and Council's RM Policy, the components of the City's Risk Management System are consistent with the *AS ISO 31000:2018 Risk Management Guidelines* (the Standard) as published by Standards Australia Limited.

4.1 THE STANDARD ON WHAT RISK IS

The Standard simply defines ***Risk*** as the effect of uncertainty on objectives.[4]

There are three (3) elements required to be identified in order to define a risk:

1. ***Objectives*** – what is the aim, goal, purpose, or strategic position to be achieved?
2. ***Uncertainty*** – what could prevent the objective from being achieved?
3. ***Effect*** – what will happen if the 'uncertainty' actually occurs? (It can be positive, negative or both, and can address, create or result in opportunities and threats)[5]

4.2 THE STANDARD ON RISK MANAGEMENT

The Standard defines ***Risk Management*** as the principles, framework and processes used to direct and control risk.[6] Figure 1 below illustrates the Standard's recommended relationship between the risk management principles, the framework and process:

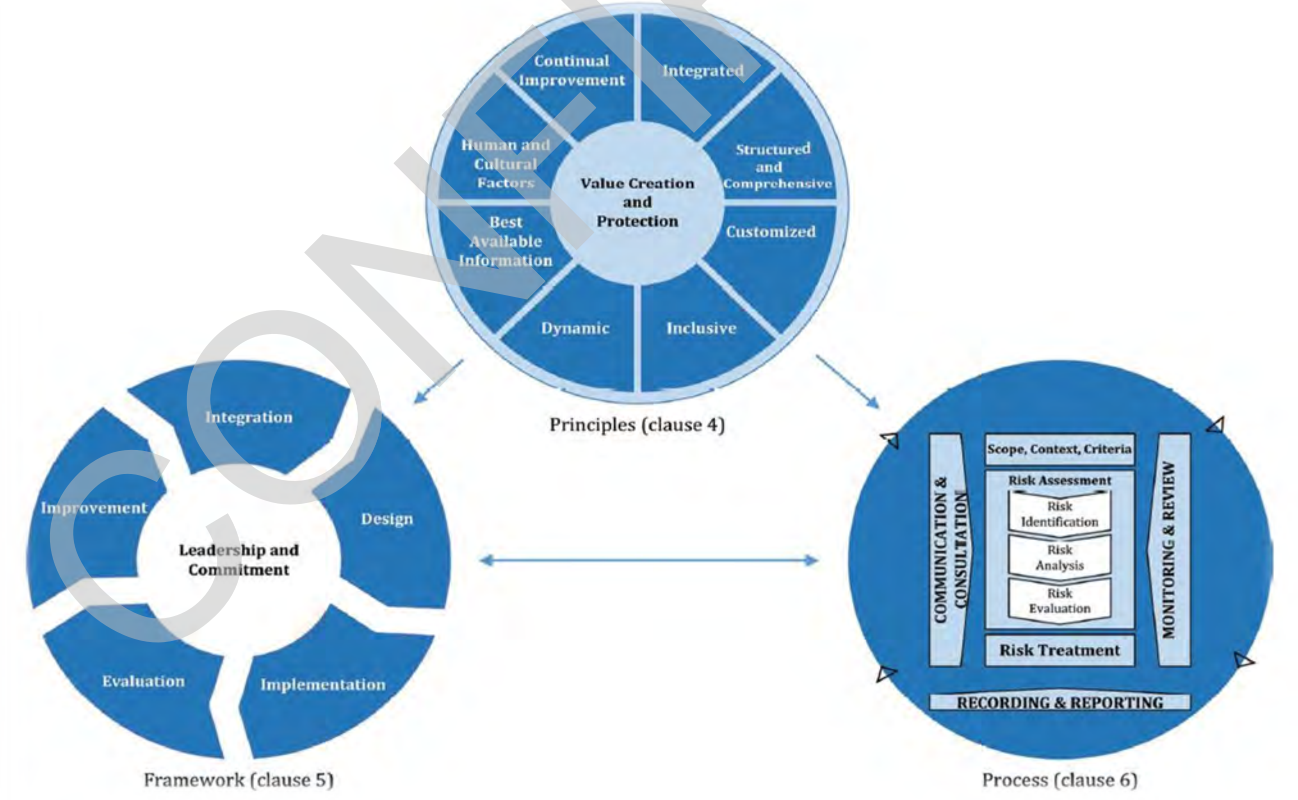


Figure 1 –AS ISO 31000:2018 recommended Risk Management System

[4] Australian ISO Standard on Risk Management: AS ISO 31000:2018, page 1.
[5] Australian ISO Standard on Risk Management: AS ISO 31000:2018, page 1.
[6] Australian ISO Standard on Risk Management: AS ISO 31000:2018, page 1.

5. Risk Management Principles

In alignment with the Standard and Council's RM Policy, the City's commitment to risk management is underpinned by the following principles.[7] All levels of the organisation will commit to incorporating these principles into their risk management activities.

5.1 PRINCIPLES

The City's risk management approach will:

A. be ***integrated*** into all management planning and operational processes undertaken or overseen by the City;

B. be a ***structured and comprehensive*** approach that is applied to ensure risk management processes are systematic and timely;

C. be ***customised*** to fit seamlessly within the City's diverse strategic, operational and project-based activities and in proportion to the external and internal context in which the City operates;

D. be ***inclusive*** of internal and external stakeholder's knowledge, views and perceptions for transparency and better-informed decision-making;

E. be ***dynamic***, ***current*** and ***responsive*** to anticipate and manage change in a meaningful and timely manner;

F. be based on the ***best available information*** considering historical, current and future expectations as would be reasonably foreseeable;

G. be the ***responsibility of all***, from Council to CEO to every employee, forming an essential element in the City's 'One Team' culture; and

H. be ***continually improved***.

Improved
Integrated
Structured
Customised
Inclusive
Dynamic
Informed
Cultural

[7] The Principles in accordance with Australian ISO Standard on Risk Management: AS ISO 31000:2018, page 3-4. Also see Figure 1. Above.

6. Council's Risk Management Policy (POL-RKM 01)

In accordance with *LGA* s2.7 Council's role is to govern the local government's affairs and be responsible for the performance of the local government's functions. As such Council has determined the RM Policy and shall satisfy itself that the City is operating an effective risk management system.

Council's RM Policy articulates the City of Mandurah's value and commitment to administrate an effective corporate-wide risk management system. The RM Policy has set the expectation that risk management is the direct responsibility of Council, the Executive Leadership Team (ELT), the Management Team (CoMMT) and staff, describing risk management as *'everyone's responsibility'*[8]. The City's RM Procedures, in conjunction with this document supports the organisation in the implementation of the RM Policy.

The RM Policy states the City's objectives of risk management as:[9]

A. ***Protection***: to safeguard the City's assets - people, financial sustainability, environment, property, reputation and information;

B. ***Improved quality***: to use risk management as a tool for improving the reliability, effectiveness and efficiency of services and infrastructure to a consistently high standard;

C. ***Increase success***: strengthen financial and non-financial outcomes by using risk assessments to make better informed decisions and clearly articulate what is achievable;

D. ***Minimise adverse impacts***: to undertake good and proper management of risks in order to prevent loss, damage and minimise harm from the City's services and infrastructure on the community, visitors and the environment; and

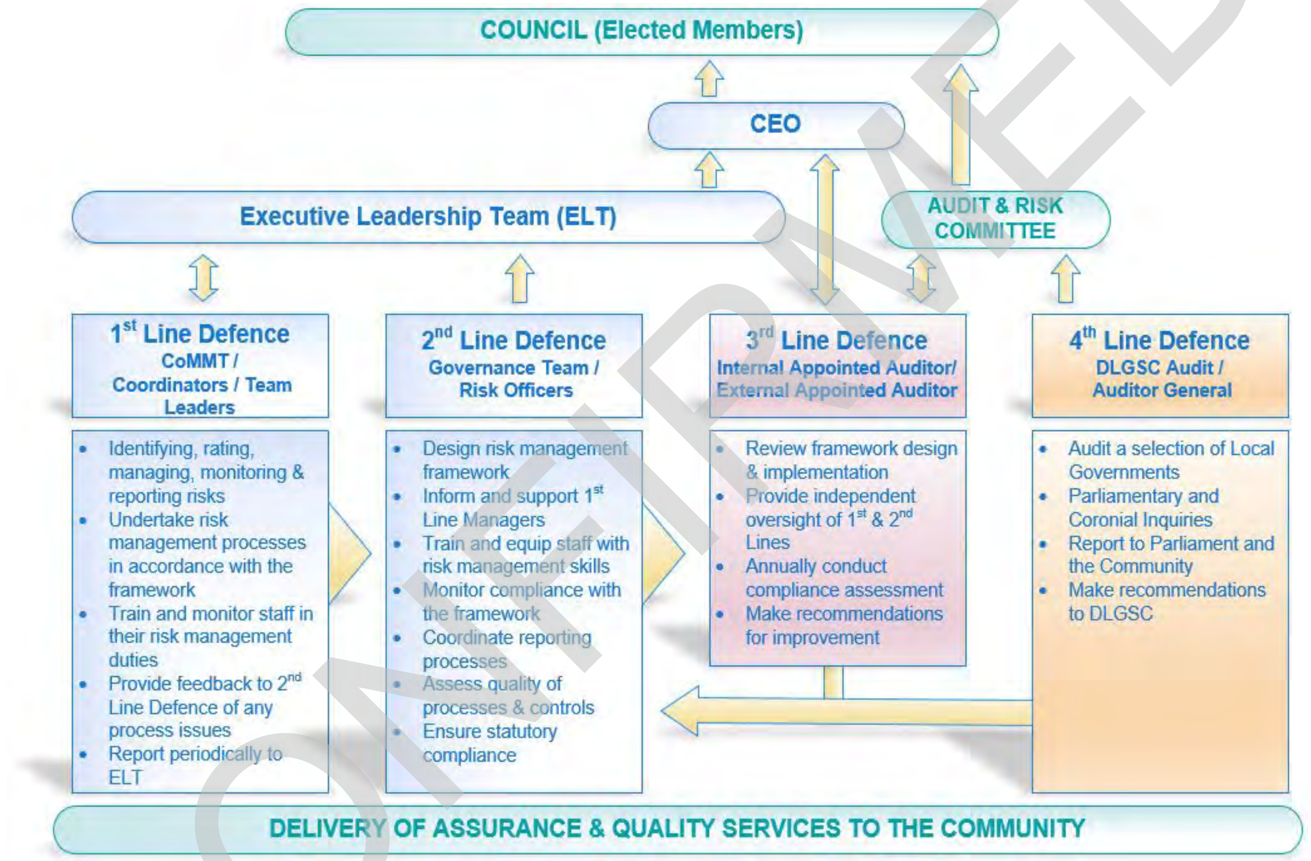
E. ***Opportunity and innovation:*** to capitalise on opportunities identified, foster creativity and facilitate innovation for future success within a sound environment.

[8] City of Mandurah (2020) *Risk Management Policy*, Council Policy POL-RKM01.
[9] City of Mandurah (2020) *Risk Management Policy*, Council Policy POL-RKM01.

7. Risk Management Assurance

The City has integrated the Office of the Auditor General (OAG) "Four Lines of Defence" model as a means of capturing and providing assurance of effective risk management.[10]

Whilst the management and reporting of risk management activities moves vertically through the organisation, the City simultaneously monitors and reviews these activities horizontally across the organisation through its Governance Services, the City's Internal Audit Function and externally appointed auditors. In doing this the City systematically enhances communications, increases transparency and strengthens control of risk management process and compliance.



COUNCIL (Elected Members)

CEO

Executive Leadership Team (ELT)

AUDIT & RISK COMMITTEE

1st Line Defence
CoMMT / Coordinators / Team Leaders

- Identifying, rating, managing, monitoring & reporting risks
- Undertake risk management processes in accordance with the framework
- Train and monitor staff in their risk management duties
- Provide feedback to 2nd Line Defence of any process issues
- Report periodically to ELT

2nd Line Defence
Governance Team / Risk Officers

- Design risk management framework
- Inform and support 1st Line Managers
- Train and equip staff with risk management skills
- Monitor compliance with the framework
- Coordinate reporting processes
- Assess quality of processes & controls
- Ensure statutory compliance

3rd Line Defence
Internal Appointed Auditor/ External Appointed Auditor

- Review framework design & implementation
- Provide independent oversight of 1st & 2nd Lines
- Annually conduct compliance assessment
- Make recommendations for improvement

4th Line Defence
DLGSC Audit / Auditor General

- Audit a selection of Local Governments
- Parliamentary and Coronial Inquiries
- Report to Parliament and the Community
- Make recommendations to DLGSC

DELIVERY OF ASSURANCE & QUALITY SERVICES TO THE COMMUNITY

7.1 FIRST LINE OF DEFENCE – City of Mandurah Management Team, Coordinators & Team Leaders

Each directorate / business area / service unit is responsible for the ownership and management of their risks. CoMMT, Coordinators and Team Leaders are the first line of assurance for risk management in the organisation and fundamental to its effectiveness through the practical performance of risk activities.

[10] Office of The Auditor General (2020) *Audit Results Report – Annual 2018-19 Financial Audits of Local Government Entities*, Western Australia, Report 16 2019:20, page 27-28.

1st Line Key activities are to:

- promote, guide and assist each member of the team to actively participate in risk management through the business area's systems and processes;
- undertake risk identifications, assessments, and evaluations within the scope of the business areas objectives;
- prepare risk acceptance proposals and plans based on the level of residual risk and Council's risk appetite;
- exercise control through the ongoing management, monitoring and review of the business area's accepted risks; and
- provide periodical reports to ELT.

7.2 SECOND LINE OF DEFENCE – Governance Services

Governance Services are responsible for the design and implementation of the framework, risk procedures and risk compliance in the organisation.

2nd Line Key Activities are to:

- provide assurance and transparency on the risk and control environment between 1st and 3rd Lines of Defence;
- train and support the 1st Line process;
- manage and monitor compliance with the risk management framework;
- consult, review and implement any changes to the risk management framework for organisational improvement; and
- coordinate the City's reporting for the CEO, ELT, Audit and Risk Committee (A&R Committee) and Council.

7.3 THIRD LINE OF DEFENCE – Internal Audit Function

The City has an established internal audit function that provides independent assurance to Council and the A&R Committee. It is an independent, objective assurance and consulting activity designed to add value and improve the City's operations. The purpose of the internal audit function is to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The City's internal audit function should evaluate and monitor the adequacy and effectiveness of the internal control framework as a minimum. Risk management is also an essential part of the City's management and internal control framework. It looks at what risks the City may face and the best way to address these risks. Assessment and management of risk is central to determining internal audit activities.

The three-year Strategic Internal Audit Plan (SIAP) provides an outline of the areas the City considers to be a priority for review, using a risk-based approach. The SIAP is based on a risk assessment of the City's key strategic and operational areas to determine the appropriate timing and frequency of coverage of each of these areas.

Internal audit service providers are engaged to conduct audits in accordance with the Strategic Internal Audit Plan 2020/21 – 2022/23, which is reviewed by A&R Committee and adopted by Council.

3rd Line Key Activities are to:

- provide an impartial assessment of the organisation's compliance with the City's legislative requirements, the risk management framework and processes;
- audit and assess specific areas as determined by the CEO with the input of the Audit and Risk Committee;
- alert the 2nd Line as to areas of lack and potential control issues; and
- provide recommendations as to framework design, internal controls and improved processes.

7.4 FOURTH LINE OF DEFENCE – Auditor General and Other External Reviews

External audits may be undertaken by the OAG, Department of Local Government, Sport & Cultural Industries or other parliamentary enquiries. The purpose of these audits is to ensure regulatory compliance and assess the City's level of integrity.

The external audit reports are presented to parliament and the community. They are a helpful information tool for local governments to stay abreast with changes, expectations and improved methods of risk management.

This 4th Line of Defence provides both the leadership and the community with assurance that the City is operating with excellence, honesty and integrity.

7.5 ASSURANCE OF AUDIT AND RISK COMMITTEE

In accordance with section 7.1A of the *LGA*, the Council has established an A&R Committee which serves as another means of assurance for the City. The A&R Committee will operate in accordance with all relevant provisions of the Act, the *Local Government (Audit) Regulations 1996* (Audit Regulations) and the *Local Government (Administration) Regulations 1996* (Administration Regulations).

As prescribed in Section 16 of the Audit Regulations the A&R Committee is to provide guidance and assistance to Council on matters relevant to its terms of reference. This role is designed to facilitate informed decision-making by Council in relation to its legislative functions and duties that have not been delegated to the CEO. In the context of risk management, the role of the A&R Committee is to:

- Monitor and receive reports concerning the development, implementation and on-going management of a City-wide risk management plan (strategic risk management);
- Receive and review reports from the CEO regarding the appropriateness and effectiveness of the City's risk management, internal controls and legislative compliance at least once every three financial years; and
- Support Council in fulfilling its governance and oversight responsibilities in relation to financial reporting, internal control structure, risk management systems, internal and external audit functions and ethical accountability.

8. Risk Appetite

The risk appetite is the amount of risk exposure that the City is prepared to accept in the pursuit of its strategic community objectives. The risk appetite for the City is determined by Council, in conjunction with the CEO.

Council have a key role to set and approve the risk appetite for each strategic risk and accordingly the organisation must operate within the established risk appetite. Risk appetite thresholds are to be reviewed by Council every two years as part of the Risk Management Framework review.

8.1 RISK APPETITE GUIDELINES

8.1.1 Once the CEO has identified, analysed, mitigated and re-evaluated the ***residual risk rating*** for each strategic risk, if the risk is moderate or above, the risk will be provided to the A&R Committee who will review the risk and the risk assessment and consider management recommendations. The A&R Committee will also review each operational risk that has a residual risk rating of high or above.

8.1.2 Factors to be considered when setting the Risk Appetite levels
In deciding the risk appetite Council and the CEO are required to consider and articulate:

- the priority order of strategic objectives;
- resources to be allocated;
- emerging risks within the City's control;
- risks outside the City's control;
- the risk tolerance levels of external and internal stakeholders;
- any legislative requirements or limits; and
- recommendations made by the A&R Committee.

8.1.3 Risk Appetite Rating
With consideration to the factors listed above, Council are to decide the maximum level of risk rating that the City will tolerate for each strategic risk. This forms the ***risk appetite*** that the City is to perform its operations within. Once adopted by Council, the CEO is responsible for ensuring the integration of the risk appetite into the organisations processes.

9. Strategic and Operational Risk Management

The RM Framework has been developed with a focus on managing risk at the strategic and operational levels. Both levels of risk are to be managed in accordance with the Standard's Risk Management Process (item 10 of this document) and have been incorporated into the City's RM Procedure. An overview of strategic and operational risks are below:

9.1 STRATEGIC RISKS

Strategic risks affect the sustainability of the City or its ability to deliver on the strategic community objectives. Strategic risks may affect the whole City, a significant part of the organisation, the longer-term interests of the City and the Community and may possibly affect future service delivery.

It is the strategic community objectives and strategic risks that shape, define, limit, qualify and quantify how the entire organisation will do business. Failure to adequately manage strategic risks could result in catastrophic consequences or put the City at risk of total failure and major loss.

Council, A&R Committee, the CEO, ELT and CoMMT all play a role in strategic risk management.

9.2 OPERATIONAL RISKS

Operational risks relate to the day-to-day operations, activities, functions and services of the organisation. Operational risks are those that affect the viability of achieving activities associated with individual business units and operational objectives. These risks include issues that affect 'business as usual' activities and the basic services of each business unit. Operational risks relate to the effective and efficient use of the City's resources, and can have a day-to-day impact on specific operations.

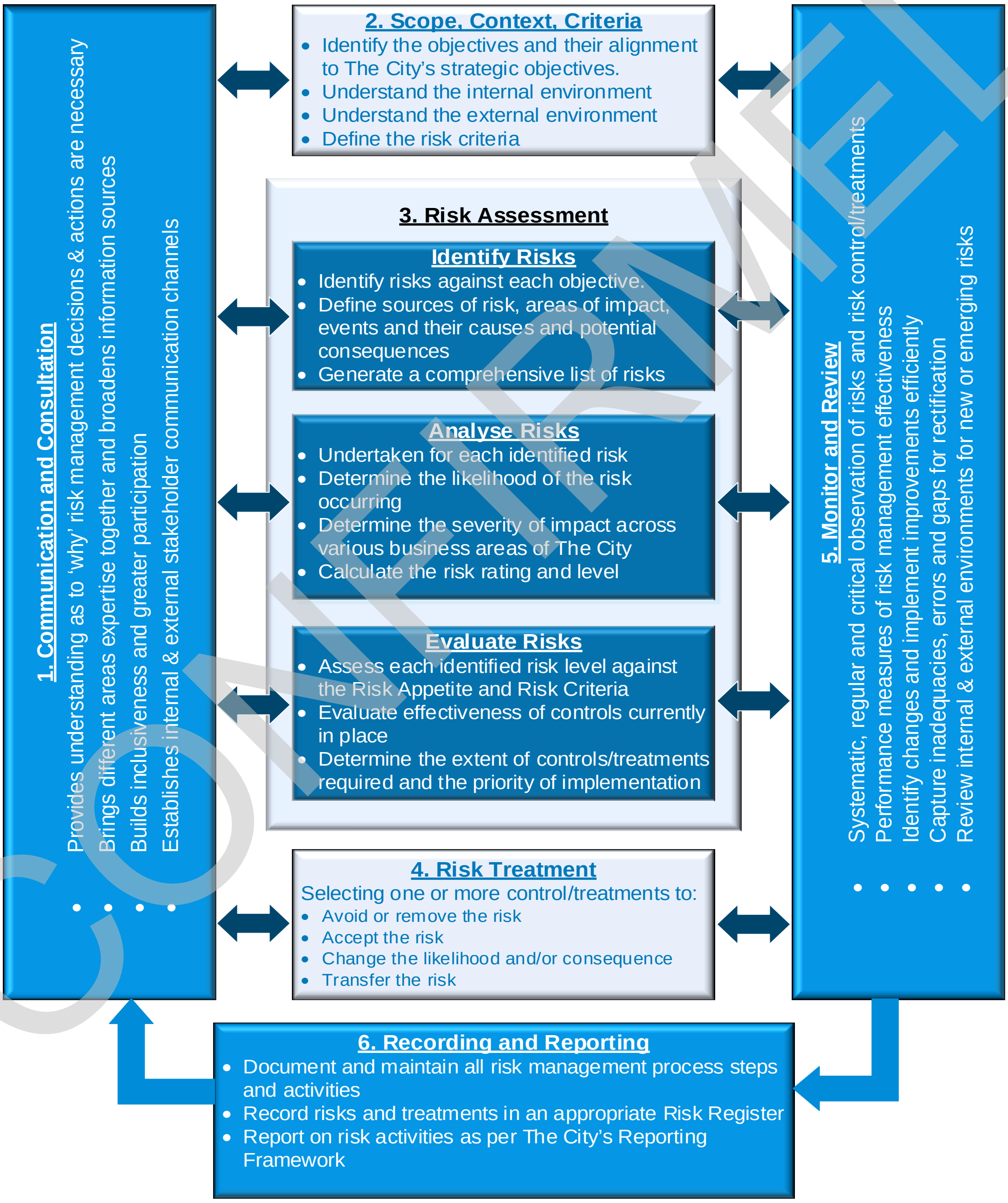
The City's strategic objectives, strategic risk assessments and treatment plans, along with the Risk Appetites as determined by Council, will inform and limit the operational objectives and management of operational risks. Business Units are to identify their work task objectives and undertake risk assessments. These risk assessments will inform, streamline and clarify how the Business Unit is to best complete its work.

Operational risks also include Project Risks. Project risks are risks associated with individual projects, initiatives or day-to-day business activities at the City. Project risks are to be assessed in the project planning phase and throughout the duration of the project's business activities.

ELT, CoMMT and Teams are responsible for operational risk management.

10. Risk Management Process

The Risk Management Process (RM Process) is the practical 'how to' component of the RM Framework and is to be integrated into the City's management practises, decision-making methods, business plans, operations and procedures for optimum results. The RM Process is standardised across all areas of the City and is documented in the City's RM Procedures. The following diagram outlines that RM Process that aligns with the Standard[11] with the following commentary providing broad descriptions of each step:



1. Communication and Consultation
- Provides understanding as to 'why' risk management decisions & actions are necessary
- Brings different areas expertise together and broadens information sources
- Builds inclusiveness and greater participation
- Establishes internal & external stakeholder communication channels

2. Scope, Context, Criteria
- Identify the objectives and their alignment to The City's strategic objectives.
- Understand the internal environment
- Understand the external environment
- Define the risk criteria

3. Risk Assessment

Identify Risks
- Identify risks against each objective.
- Define sources of risk, areas of impact, events and their causes and potential consequences
- Generate a comprehensive list of risks

Analyse Risks
- Undertaken for each identified risk
- Determine the likelihood of the risk occurring
- Determine the severity of impact across various business areas of The City
- Calculate the risk rating and level

Evaluate Risks
- Assess each identified risk level against the Risk Appetite and Risk Criteria
- Evaluate effectiveness of controls currently in place
- Determine the extent of controls/treatments required and the priority of implementation

4. Risk Treatment

Selecting one or more control/treatments to:
- Avoid or remove the risk
- Accept the risk
- Change the likelihood and/or consequence
- Transfer the risk

5. Monitor and Review
- Systematic, regular and critical observation of risks and risk control/treatments
- Performance measures of risk management effectiveness
- Identify changes and implement improvements efficiently
- Capture inadequacies, errors and gaps for rectification
- Review internal & external environments for new or emerging risks

6. Recording and Reporting
- Document and maintain all risk management process steps and activities
- Record risks and treatments in an appropriate Risk Register
- Report on risk activities as per The City's Reporting Framework

[11] See also Risk Management System Diagram - Figure 1. page 4.

10.1 STEP ONE - COMMUNICATION & CONSULTATION

Communication and consultation are imperative to the effectiveness of risk management and are to be factored into each step of the process.

10.1.1 COMMUNICATION

Communication ensures that those responsible for risk management activities and any affected internal and external stakeholders understand why certain decisions are made and actions taken.[12] Effective communication strengthens, simplifies and unites risk management processes.

10.1.2 CONSULTATION

Consultation enriches and improves risk management decisions, activities and outcomes. Consultation allows for the consideration of different areas of expertise, different viewpoints, feedback and broader information. It encourages inclusiveness and builds a greater sense of ownership for those affected by risk decisions and actions.

10.2 STEP TWO - SCOPE, CONTEXT & CRITERIA

An important step in the risk management process is understanding the context within which risks are to be addressed. Establishing the scope, context and criteria allows the risk management processes to be customised to the City's policies and procedures.[13] It also enables different business areas, teams and projects to treat and successfully manage risks in ways that are relevant to their business operations.

10.2.1 SCOPE

It is important to define the scope of risk management activities in order to keep the process efficient and effective. When defining scope consideration should be given to the following:

- the objectives and how they align with the City's strategic objectives;
- the expected outcomes from this RM Process;
- time, location and budget restrictions;
- risk assessment tools, techniques and any existing risk profiles;
- available resources, persons responsible and records to be kept; and
- the relationship with other business areas, projects, processes and activities.

10.2.2 EXTERNAL CONTEXT

Understanding the external factors that may impact or be impacted by the City's risk management activities is necessary in order to ensure the Community and external

[12] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 9.
[13] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 10.

stakeholders are considered. The external context to be considered may include, but is not limited to:

- Social, political, regulatory, economic, financial, technological and environmental factors;
- Community, Industry, Regional, State, National and International expectations and trends;
- External Stakeholder and strategic third-party relations;
- The City's external threats and opportunities;
- Health and safety requirements; and
- Media and publicity factors.

10.2.3 STRATEGIC AND INTERNAL CONTEXT

It is equally as important for every member of staff to have a good understanding of the City as an organisation. The more informed staff are the more the City performs as 'One Team'. Internal factors to be considered are:

- City of Mandurah's community vision;
- City's strategic objectives;
- Integrated Planning and Reporting;
- 'One Team' Culture;
- Regulatory requirements and contractual obligations;
- CEO Policies and procedures;
- Occupational Safety, Health and Wellbeing ('OSH');
- Codes of Conduct;
- Organisational structure and governance;
- City's internal strengths, weaknesses opportunities and threats (SWOT); and
- Internal Stakeholders.

10.2.4 RISK CRITERIA

The risk criteria are the City's standards against which all risks are measured and evaluated. This is set out in Annexures 1 - 4. The level of detail that will be entered during the risk management process will be determined by the risk appetite threshold for that particular activity and the nature of the residual level of risk. In each instance consideration must always be given to the strategic objective that the activity supports and the budget allocated to it.

10.3 STEP THREE - RISK ASSESSMENT

In accordance with the Standard, a risk assessment is the overall process of ***risk identification***, ***risk analysis*** and ***risk evaluation*** undertaken within the parameters of the defined scope, contexts and criteria.[14] Risk assessments are not scientific. They are based on the best available information and require a common-sense approach. Risk assessments should form part of any strategic, business, team, project or operational plan. They are to be undertaken systematically, recurrently and in collaboration with stakeholders.

Strategic Risk Assessments are to be completed annually with corporate planning and Operational Risk Assessments for each Directorate should also be done annually as a minimum. Any 'out of cycle' risk assessments will also be required to be undertaken when events arise, audit or review recommendations are made or a material change occurs.

10.3.1 RISK IDENTIFICATION

Risks are the potential of something happening - a possibility and not an actuality. Actual past events locally, nationally and globally often assist in determining risks. Once risks have been named, additional information as to 'when', 'why' and 'how' must also be identified for each risk.

Identification of risks, whether in the City's control or not, must be comprehensive as failure to do so can have costly financial (losses, penalties, costs, fines, etc.) and non-financial (community harm, damage to reputation, damage to assets, regulatory enforcement, business interruption, legal claims, etc.) impacts or could result in lost opportunities for the City.

The City may use a range of tools and techniques to identify risks, including:

- facilitated focus group (ad-hoc) brainstorming sessions;
- specialist team working group reviews (departmental focus);
- multi-disciplinary, multi-factorial project risk review workshops;
- SWOT analysis, process mapping, flow charting, systems analysis or operational modelling;
- Strategic, planning, budget and risk identification workshops;
- Examination and review of past reports and events;
- Compliance audits and reviews; and
- OSH techniques such as Job Safety Analysis (JSA) and Safe Work Method Statement (SWMS).

Identified risks are to be documented in one of the appropriate ***Risk Registers***.

[14] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 11.

Risk events, their cause and effect are to be recorded and grouped by the risk source. For example:

- external theft and fraud;
- misconduct;
- business and community disruption;
- errors, omissions and delays;
- failure of IT or systems and infrastructure;
- failure to fulfil statutory regulations or compliance requirements;
- providing inaccurate advice/ information;
- inadequate project/change management;
- inadequate document management processes;
- inadequate safety and security practices;
- inadequate engagement practices;
- inadequate asset sustainability practices;
- inadequate supplier/contract management;
- ineffective employment practices;
- ineffective management of facilities/venues/events; or
- inadequate environmental management.

10.3.2 RISK ANALYSIS

The primary purpose of a risk analysis is to provide a measure of the ***Risk Likelihood*** and ***Risk Impact*** for each identified risk. These are multiplied together to equal the overall ***Risk Rating***.

Risk Likelihood X *Risk Impact* = *Risk Rating*

Risk Analysis is completed in three steps and at two (2) separate stages

The risk analysis is completed for every risk listed in the Risk Identification process and is undertaken at two (2) separate stages throughout the RM Process. The first stage is the ***Inherent Risk Analysis*** and the second stage is the ***Residual Risk Analysis***.

STAGE 1 - Inherent Risk Analysis

Risk assessments on an inherent basis assumes that no risk controls are in place or that all or a substantial part of the controls have failed. This allows the City to understand which risks have the most potential to adversely affect it or its operations and require strong controls and greater oversight. The Inherent Risk Analysis is undertaken immediately after the Risk Identification process.

STAGE 2 - Residual Risk Analysis

A residual risk analysis is a re-assessment of the identified risks taking into consideration any controls that are in place or to be put in place. The effectiveness of those controls will determine if there is any reduction in the residual risk rating when compared to the inherent risk rating. A Residual Risk Analysis is undertaken after the Inherent Risk Rating has been evaluated and controls/treatments to mitigate or reduce the risk level have been applied.

Three (3) Steps of Risk Analysis:

STEP 1 - Risk Likelihood

The likelihood is the probability and frequency of a risk occurring. The City uses the below table[15] to rate the likelihood of the risk from 1 to 5. This is called the ***Likelihood Rating*** and is required to determine the overall risk rating.

STAGE 1 - Inherent Risk Likelihood - the probability and frequency of the risk occurring based on the assumption that no controls are in place or if the controls have failed.

STAGE 2 – Residual Risk Likelihood – the probability and frequency of the risk occurring taking into consideration the effectiveness of existing controls in place.

Rating	Description	Likelihood / Probability of Occurrence	
5	Almost Certain	The event could occur in most circumstances	More than 3 times per year
4	Likely	The event is expected to occur	1-2 times per year
3	Possible	The event will possibly occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

STEP 2 – Risk Impact

The Risk Impact is the severity or consequence of the risk occurring. The City recognises seven (7) different areas (does not include project risk area) of potential impact and rates it against five (5) levels of impact severity. A risk consequence may affect more than one area and have differing levels of severity. Management will be required to decide which area of impact has the highest consequence and which business area is therefore, best responsible for management of that risk.

The City's **Risk Impact Table** is in Annexure 2. It is used to determine each risk's ***Impact Rating*** of 1 to 5.

[15] See also 'Risk Likelihood Rating Table' in Annexure 1.

STAGE 1 - Inherent Risk Impact - the level of severity and consequence that the risk may cause based on the assumption that no controls are in place or if controls fail.

STAGE 2 – Residual Risk Impact – the level of severity and consequence the risk may cause taking into consideration the effectiveness of existing controls in place.

The City's has recognised the main **areas of risk impact** are:

- Health
- Financial Impact
- Service Interruption
- Compliance
- Reputational – External & Internal
- Property
- Environment
- Projects – Time & Cost

The City's **levels of impact severity and numerical rating** are:

Catastrophic	5
Major	4
Moderate	3
Minor	2
Insignificant	1

STEP 3 - Risk Rating

Every identified risk is to be given an overall ***Risk Rating*** using **The City of Mandurah's Risk Rating Chart**[16] shown below. The risk rating is calculated by multiplying the *Likelihood Rating* by the *Impact Rating*. The higher the number the more critical the risk. The risk rating will determine which level the risk is categorised into and the extent to which it is to be controlled, monitored and reviewed.

The risk rating levels are:

1 – 2	= Negligible	**5 - 9**	=Medium	**20 – 25**	= Extreme
3 - 4	= Low	**10 - 19**	= High		

STAGE 1 - Inherent Risk Rating –
Inherent Likelihood Rating X Inherent Impact Rating = Inherent Risk Rating

The Inherent Risk Rating is then categorised into one of the above risk levels. This is called the ***Inherent Risk Level***.

STAGE 2 – Residual Risk Rating –
Residual Likelihood Rating X Residual Impact Rating = Residual Risk Rating

[16] See also 'The City of Mandurah's Risk Rating Chart' Annexure 3.

The Residual Risk Rating is then categorised into one of the above risk levels. This is called the ***Residual Risk Level***.

THE CITY OF MANDURAH RISK RATING CHART

Likelihood Rating **X** ***Impact Rating*** **=** ***Risk Rating***

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Medium	10 High	15 High	20 Extreme	25 Extreme
Likely 4	4 Low	8 Medium	12 High	16 High	20 Extreme
Possible 3	3 Low	6 Medium	9 Medium	12 High	15 High
Unlikely 2	2 Negligible	4 Low	6 Medium	8 Medium	10 High
Rare 1	1 Negligible	2 Negligible	3 Low	4 Low	5 Medium

Impact →

Likelihood ↑

10.3.3 RISK EVALUATION

Risk evaluation involves comparing the level of risk found during the analysis process with The City's risk criteria for treatment and risk appetite thresholds.[17] It is the primary source of information on which effective risk management decisions are based.

Risks that fall within acceptable limits may simply need to be acknowledged and monitored, while other risks in higher levels may have the potential to threaten the City's strategic and operational objectives and require treatment.

Risk evaluation enables the City to tally the number of identified risks within each level. This will aid the City in recognising associated risks, any high impact zones or gaps in the City's organisational control measures. For example, multiple minor issues associated with a particular task, project or business area, whilst not significant in and of themselves, when combined pose a much higher risk.

Risk Evaluation at each Stage:

STAGE 1 - Inherent Risk Evaluation –
The ***Inherent Risk Level*** provides the City with an understanding of the raw level of effect a risk may cause should it occur without controls or if controls fail. The Inherent Risk Level must be evaluated against the appropriate ***Risk Appetite*** threshold and the below table:

Inherent Risk Level Action

Extreme 20 - 25	High 10 - 19	Medium 5 – 9	Low 3 – 4	Negligible 1 - 2
• Treatment is urgently required	• Treatment required	Decided on a case by case basis – • Treat to see if level can be reduced; or	Decided on a case by case basis – • Treat to see if level can be reduced; or	• Capture as a part of compliance requirements

[17] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 12.

		• accept as is & monitor	• accept as is & monitor	

STAGE 2 – Residual Risk Evaluation –
The ***Residual Risk Level*** provides the City with direction as to what responses it is required to undertake in management and monitoring of the risk. The residual risk level should be within Council's ***Risk Appetite*** threshold. If it is not, then further treatment is required and an additional risk analysis is to be completed until it is within the acceptable level of exposure. The below table indicates what action is to be taken next:

Residual Risk Level Action				
Extreme 20 - 25	**High 10 - 19**	**Medium 5 – 9**	**Low 3 – 4**	**Negligible 1 - 2**
• More treatment is urgently required	Decided on a case by case basis – • more treatment required; or • accept with ELT strict & regular monitoring	Decided on a case by case basis – • accept & monitor; or • more treatment required	• Accept & monitor – no further treatment required	• Accept & monitor – no further treatment required • May form a part of compliance requirements

10.4 STEP 4 - RISK CONTROLS/TREATMENTS

Risk control/treatment is the implementation of response actions to reduce the likelihood and/or negative impact of a risk. The Risk Appetite sets the maximum level of risk exposure that the City is prepared to accept. Risk control/treatments enables the City to safely and intelligently pursue its objectives in the face of potential risks and within the limits of the Risk Appetite.

The Standard advises that risks may be able to be controlled/treated by one or more of the following approaches:[18]

- avoiding the risk by not pursuing the activity that give rise to it;
- increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood of the risk occurring;
- changing the impact of the risk;
- sharing the risk with other parties; and
- accepting the risk by informed decision.

10.4.1 APPLICATION OF CONTROLS/TREATMENTS AT THE DIFFERENT STAGES

STAGE 1 – Inherent Risk Level
Risk controls are firstly applied to the Inherent Risk Level. As stated above, the Inherent Risk Level is the rating of the raw risk without any controls/treatments in place. It is expected that

[18] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 13.

once existing controls are assessed that manage the risk then the Stage 2 Risk Analysis will report a lower risk level. This is known as the Residual Risk Level.

STAGE 2 – Residual Risk Level
If the Residual Risk Level is not within the Risk Appetite threshold then further controls/treatments are required and an ***Action Plan*** must be developed until the Residual Risk Level has been reduced.

Once the action plan has been implemented, the residual risk level should be recalculated based on the improved controls that are now in place. Note: There may be in some instances, that the residual risk level will remain the same even with improved controls.

10.4.2 DIFFERENT CONTROL/TREATMENT OPTIONS[19]

The City has several different control/treatment options and more than one may be applied to a risk. Some controls are intended to prevent a risk event, detect an event or respond to a risk event.

Accept the risk

A risk may be accepted if:

- the risk level rating is low or negligible;
- the community benefit outweighs the cost of treating the risk;
- the risk is within the appropriate Risk Appetite threshold; or
- The City has limited or no control over the risk. E.g. natural disasters, pandemics, international economic impacts or terrorist attacks. The City is to have emergency, recovery and business continuity plans in place to manage and recover from such risks.

Transfer the risk

A risk may be transferred partly or wholly to a third party. Whilst this may be a cost-effective way to reduce the risk level a certain degree of the original risk will always remain and a new risk of being dependant on a third party is inherited. The City may transfer risk through:

- Insurance;
- Terms of contract – limited liability clause or waiver of liability; or
- Compensating a third party to take on management of the risk.

Eliminate the risk

Eliminating the risk is only achieved by avoiding or discontinuing the activity. For Low level risks this may be as simple as altering an organisational process and turning it into a compliance requirement. For Extreme or High level risks that cannot be reduced to an acceptable level, it

[19] Control/Treatment options have been gleaned from a wide variety of sources including: Australian ISO Standard on Risk Management: AS ISO 31000:2018; Insurance Commission of Western Australia, '*Risk Management Guidelines',* accessed April 2020 at https://www.icwa.wa.gov.au/government-insurance/risk-management; and The Institute of Internal Auditors Australia (January 2019) '*Control Assessment: A Framework*', Sydney NSW.

may require the City to re-think its plans, projects and even its objectives. An objective or activity may need to be altered, delayed or scrapped entirely. Eliminating an Extreme or High level operational risk will usually require ELT approval. Eliminating an Extreme or High level strategic risk will require approval from the CEO and Council (through the Audit and Risk Committee).

Controls

Types of controls are set out in the table below:

Directive controls Directive controls exercise a power or authority to establish a desired outcome: • Council policies, CEO policies, codes of conduct and procedures; • Creating laws and regulations; • Setting limits, thresholds or standards; • Training and equipping seminars; • Job descriptions; or • Meetings.	**Preventative controls** Preventative controls reduce and discourage irregularities: • Organisational/Directorate/Business Area processes; • IT access authorisations and passwords; • Segregation of duties; • Fines and penalties; • Review and approval systems; • Internal audit functions; • Physical control over assets; • Warnings and signs, physical barriers; • Stakeholder management and engagement strategies; or • Asset Maintenance strategies
Detective controls Detective controls find issues and irregularities after they have occurred: • Financial reconciliations; • Inventory stocktakes; • Comparison reports and reviews; • Alarms; • IT alerts; or • Audits.	**Corrective controls** Corrective controls mitigate the extent of any damage caused by a risk event: • Reporting and noting a correction upon discovery of an error; • Updating and improving a process or procedure; • Anti-virus software; • System upgrades; • Additional training; • Increase supervision; or • Recovery Plans.

10.4.3 SELECTING THE MOST APPROPRIATE CONTROL & TREATMENT

Selecting the most appropriate control/treatment must always be with the operational and strategic objectives in mind. Risk treatments are to be considered in priority of effectiveness and efficiency to ensure adequate resources can be allocated and the desired outcome is achieved.

Consideration should be given to the following when deciding the most appropriate treatment to implement:

- How will the treatment modify the risk level?

- Do the costs of the treatment justify the benefit?
- How compatible is the treatment with the business objective and over-arching strategic objective?
- Does the treatment contradict or compliment any existing risk treatment activities?
- Does the treatment comply with legislation?
- Does the treatment create new or secondary risks?
-

10.4.4 IMPLEMENTING CONTROLS & TREATMENTS

Treatments and controls may be implemented within a team, business area, directorate or across the whole organisation. They may also be dependent on different business areas working together to ensure effectiveness and efficiency. For example, IT may be relied upon to ensure systems are available to manage a treatment.

Risk treatments must be assigned to a person/s who will be responsible for implementing, managing and reviewing risk levels and controls. ELT will be accountable for oversight of strategic risk treatments and CoMMT will be accountable for oversight of operational risk treatments. The City's Roles and Responsibilities can be found in item 11.

Action Plans

An Action Plan must be developed where controls and treatments are weak or inadequate and further mitigation is required. For example, if the Residual Risk Level is not within the Risk Appetite Threshold.

Action Plans are to be:

- **Assigned** – person responsible for ensuring the action is implemented
- **Specific** – state the exact activities to be implemented and the required resources
- **Timely** – must be completed within appropriate timeframes
- **Achievable** – action and activities must be practicable and state any restrictions
- **Measurable** – the action must be able to be assessed
- **Justified** – evidence of actual reduction in the Residual Risk Level
- **Monitored** – tracked, managed and reported.

Audits may be undertaken to ensure Action Plans are on track, remain relevant or have been successfully completed and closed out.

10.5 STEP 5 - MONITOR & REVIEW

The Standard emphasises that effective risk management is attained through ongoing and periodic monitoring and reviews at every stage throughout the RM Process.[20] The City of Mandurah and its internal and external environments are fluid. Regular monitoring and reviews enable the City to quickly adapt and respond whilst maintaining effective risk control activities.

Risk monitoring and reviews will primarily be the responsibility of those assigned to manage the risk. Identified risks, their controls and any action plans are able to be reviewed in the ***Risk Register*** and a summary of the City's risk exposure can be monitored through ***Risk Profile***. Currently, the City uses software to host its risk management data.

Certain areas of the City will assist with monitoring and reviewing the appropriateness of identified risks, risk levels and risk treatments:

- Changes in strategic objectives;
- New legislation and regulations;
- IT outages;
- Complaints;
- Reported incidents;
- Internal and external audits; and
- Completed projects.

Risk control/treatments must be monitored and reviewed to assess their effectiveness as this may alter the level of a risk. The following table provides a basis for rating a control/treatment:[21]

EXISTING CONTROLS RATINGS		
Rating	**Foreseeable**	**Description**
Effective	There is little scope for improvement.	Processes (Controls) operating as intended and aligned to Policies / Procedures. Subject to ongoing monitoring. Reviewed and tested regularly.
Adequate	There is some scope for improvement.	Processes (Controls) generally operating as intended, however inadequacies exist. Limited monitoring. Reviewed and tested, but not regularly.
Inadequate	There is a need for improvement or action.	Processes (Controls) not operating as intended. Processes (Controls) do not exist, or are not being complied with. Have not been reviewed or tested for some time.

[20] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 14.

[21] 'The City of Mandurah's Control/Treatment Rating Table' has been adapted from: Insurance Commission of Western Australia, '*Risk Management Guidelines*', accessed April 2020 at https://www.icwa.wa.gov.au/government-insurance/risk-management; and The Institute of Internal Auditors Australia (January 2019) '*Control Assessment: A Framework*', Sydney NSW.

The City's implementation of the Four Lines of Defence Model[22] as per item 7 is another monitoring and review mechanism that the City utilises for greater assurance of effectiveness of risk management activities.

[22] See Item 7. above.

10.6 STEP 6 - RECORDING & REPORTING

The Standard advises that Risk management process and their outcomes must be documented and reported in order to:[23]

- communicate risk management activities across the organisation and with stakeholders;
- improve risk management processes and build from acquired information and experience;
- provide evidence of risk management activities for legal and auditing purposes; and
- be accountable for risk management responsibilities.

The City's RM Process requires recording and reporting risk management activities across three (3) platforms:

10.6.1 THE CITY'S RISK REPORTING FRAMEWORK

DOCUMENT NAME	AUTHOR	RECEIPIENT/ FINAL APPROVAL	TIMEFRAME
RISK MANAGEMENT SYSTEM			
Risk Management Policy	Manager Governance Services Governance, Risk and Compliance Officer (GRCO)	Council A&R Committee	Biennially
Risk Management Framework	Manager Governance Services GRCO	Council (noting) A&R Committee (noting) CEO & ELT	Council - biennially CEO – as required
Strategic Internal Audit Plan 2020/21 – 2022/23 Audit area: CEO Risk Management, Internal Controls and Legislative Compliance Audit (Audit Reg 17)	Chief Audit Executive Manager Governance Services	Council A&R Committee CEO and ELT	Triennial in accordance with the Strategic Internal Audit Plan 2020/21 – 2022/23

[23] Australian ISO Standard on Risk Management: AS ISO 31000:2018 page 14-15.

DOCUMENT NAME	AUTHOR	RECEIPIENT/ FINAL APPROVAL	TIMEFRAME
STRATEGIC RISK MANAGEMENT			
Strategic Risk Assessment Strategic Risks with residual rating ≥ Moderate and Operational Risks with a residual risk rating ≥ High	CoMMT ELT GRCO	A&R Committee CEO	Council – annually Reviewed Quarterly
Risk Appetite Thresholds	CoMMT ELT	Council A&R Committee CEO	Council - biennially
Strategic Risk Treatment Action Plans for ≥ High (e.g Business Continuity Plan, Emergency Plans)	CoMMT GRCO	CEO & ELT A&R Committee	Annually
OPERATIONAL RISK MANAGEMENT			
Operational Risk Assessments	CoMMT GRCO	ELT	Annually Monthly review of ≥ Moderate Risks
Operational Risk Management Process & Procedures Review	Managers, Coordinators, Team Leaders with task/project oversight GRCO	CoMMT	Annually
Operational Risk Treatment reviews	Managers, Coordinators, Team Leaders with task/project oversight GRCO	ELT CoMMT A&R Committee	Quarterly
Operational Risk Summary Reports	Managers, Coordinators, Team Leaders with task/project oversight	CoMMT ELT	Monthly Annually

10.6.2 RISK REGISTERS AND RISK PROFILE

The City uses Risk Registers to capture, manage, monitor, review, update and report on identified risks and the actions undertaken to manage them. The City's Risk Registers are subject to change as it reviews, improves and tailors its recording and monitoring processes to better suit its needs. Oversight of the Risk Registers is undertaken by the Governance Services.

Currently, The City operates a Strategic Risk Register and an Operational Risk Register that is able to report the City's Risk Profile which enables CoMMT and ELT to monitor the City's overall level of risk exposure.

10.6.3 DIRECTORATE / BUSINESS AREA / TEAM RISK MANAGEMENT RECORD KEEPING PROCESSES

The City expects that each Directorate, Business Area, Team and Project will document and maintain all their risk process and management activities. Summary reports are to be prepared monthly which will encourage good record keeping. Governance Services may review and audit risk processes and reports to ensure compliance with the RM Framework and effectiveness.

11. Roles and Responsibilities

The CEO is ultimately responsible and accountable for ensuring risk is effectively managed across the entire organisation. The CEO is supported by the ELT and CoMMT in achieving this.

In accordance with Council's RM Policy, it is the organisation's leaders who set this 'tone from the top'. The City aims to create a risk aware, but not risk adverse culture that ensures the best outcome for the City and the Community.

Risk should not be seen as a standalone function, but rather risk management should form part of the organisational culture and be factored into every decision making process at the City through the application of the Risk Management Process (refer to item 10) and the City's RM Procedures .

An overview of the roles and responsibilities in the context of risk management are set out below.

- **Council and Audit and Risk Committee** – have a key leadership role in the development and endorsement of the Risk Management Policy and determining the Risk Appetite. The A&R Committee provides recommendations to Council on matters of strategic risk, assurance, oversight, monitoring and reporting.
- **CEO and ELT** – collectively accountable for operational risk management oversight. Individually accountable for the management of the Operational Risk Register and risk treatments. Responsible for approving and monitoring risk and any operational risks with a residual risk rating ≥ Moderate.
- **CoMMT** – collectively responsible for operational risk management. Individually responsible for identifying, assessing and managing each Business Area's operational risks.
- **Team Members** – responsible for actioning risk management processes in their area of work and supporting their manager/coordinator/team leader in identifying, assessing and recommending suitable plans for managing their relevant operational risks. Responsible for immediately reporting to their manager/coordinator/team leader if any material changes occur.
- **Governance Services** – will provide support and advice to the organisation with strategic and operational risk management. Assist managers/coordinators/team leaders through the development of RM Procedures, Risk Management Guidelines and responsible for the development and delivery of a Risk Education and Training Strategy for the organisation. Monitor and review the reporting of strategic and operational risks.

Refer to Annexure 5: Roles and Responsibilities Diagram for detailed information.

12. Annexures

12.1 ANNEXURE 1: THE CITY'S RISK LIKELIHOOD RATING TABLE

Rating	Description	Likelihood / Probability of Occurrence	
5	Almost Certain	The event will occur in most circumstances	More than 3 times per year
4	Likely	The event is expected to occur	1-2 times per year
3	Possible	The event will possibly occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

STAGE 1 - Inherent Risk Likelihood - probability and frequency of the risk occurring based on the assumption that no controls are in place or if controls fail.

STAGE 2 – Residual Risk Likelihood – probability and frequency of the risk occurring taking into consideration the effectiveness of controls in place.

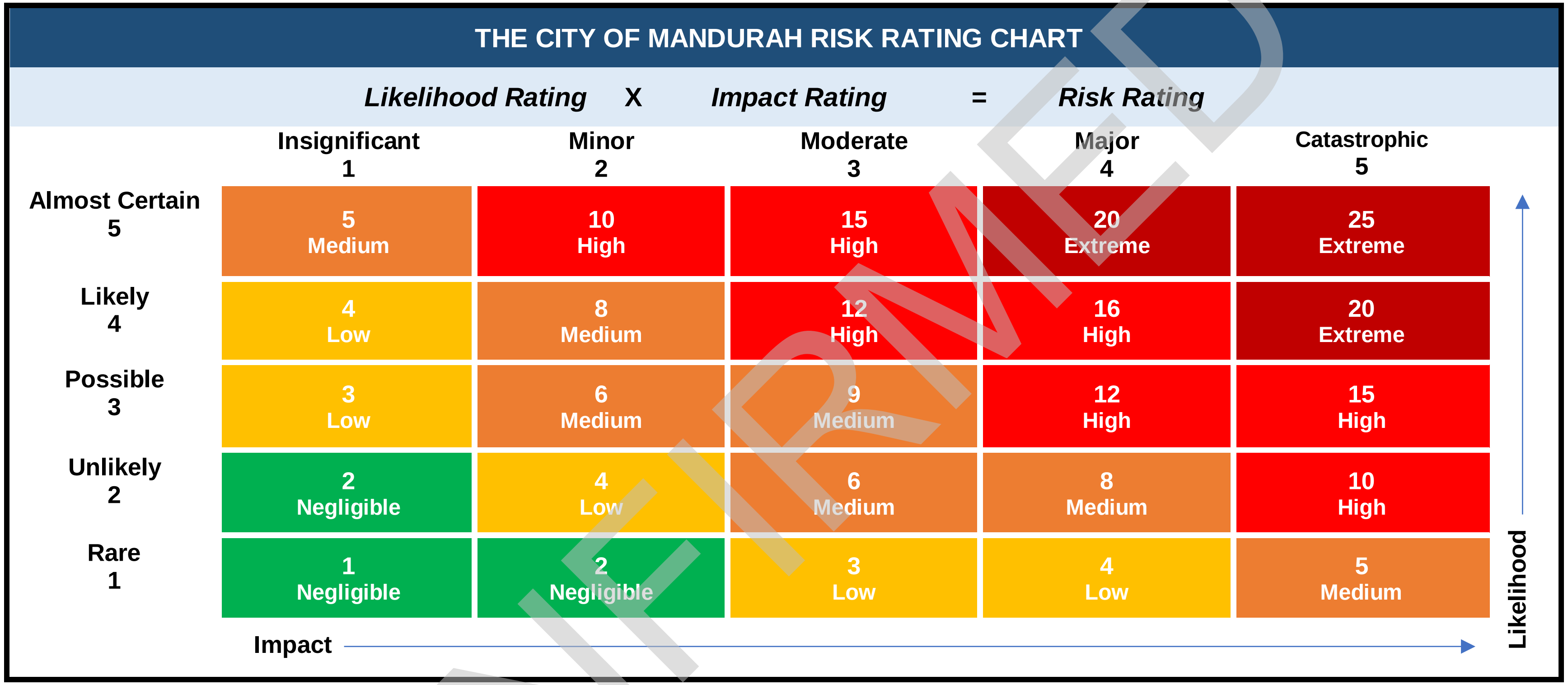
12.2 ANNEXURE 2: THE CITY'S RISK IMPACT TABLE

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Health	Near miss. Minor first aid injuries, not requiring further medical treatment	Minor injuries requiring medical treatment but not hospitalisation	Lost time injury <30 days	Lost time injury >30 days	Fatality, permanent disability
Financial Impact	Less than $50,000	$50,001 - $100,000	$100,001 - $500,000	$500,001 - $3,000,000	More than $3,000,000
Service Interruption	No material service interruption	Short term temporary interruption – backlog cleared < 1 day	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Prolonged interruption of services – additional resources; performance affected < 1 month	Indeterminate prolonged interruption of services – non-performance > 1 month
Compliance	No noticeable regulatory or statutory impact	Some temporary non-compliances	Short term non-compliance but with significant regulatory requirements imposed	Non-compliance results in termination of services or imposed penalties	Non-compliance results in litigation, criminal charges or significant damages or penalties
External Reputation	Unsubstantiated, low impact, low profile or 'no news' item	Substantiated, low impact, low news item	Substantiated, public embarrassment, moderate impact, moderate news profile	Substantiated, public embarrassment, high impact, high news profile, third party actions	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions

12.2 ANNEXURE 2: THE CITY'S RISK IMPACT TABLE

		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Internal Reputation		Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of 5% Increase in staff turnover and absenteeism of <5%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of >5% but <10% Increase in staff turnover and absenteeism of >5% but <10%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of >10% but <15% Widespread employee dissatisfaction resulting in Staff Satisfaction rating drop of <5% Increase in staff turnover and absenteeism of >10% but <15%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of >15% Widespread employee dissatisfaction resulting in Staff Satisfaction rating drop of >5% but <10% Increase in staff turnover and absenteeism of >15% but <25%	Widespread employee dissatisfaction resulting in Staff Satisfaction drop of >10% Increase of staff turnover and absenteeism of >25%
Property		Inconsequential damage.	Localised damage rectified by routine internal procedures	Localised damage requiring external resources to rectify	Significant damage requiring internal & external resources to rectify	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building
Environment		Contained, reversible impact managed by on site response	Contained, reversible impact managed by internal response	Contained, reversible impact managed by external agencies	Uncontained, reversible impact managed by a coordinated response from external agencies	Uncontained, irreversible impact
Project Risks	Time	Exceeds deadline by 10% of project timeline	Exceeds deadline by 15% of project timeline	Exceeds deadline by 20% of project timeline	Exceeds deadline by 25% of project timeline	Exceeds deadline by 30% of project timeline
	Cost	Exceeds project budget by 10%	Exceeds project budget by 15%	Exceeds project budget by 20%	Exceeds project budget by 25%	Exceeds project budget by 30%

12.3 ANNEXURE 3: THE CITY'S RISK RATING CHART



THE CITY OF MANDURAH RISK RATING CHART

Likelihood Rating X *Impact Rating* = *Risk Rating*

	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Medium	10 High	15 High	20 Extreme	25 Extreme
Likely 4	4 Low	8 Medium	12 High	16 High	20 Extreme
Possible 3	3 Low	6 Medium	9 Medium	12 High	15 High
Unlikely 2	2 Negligible	4 Low	6 Medium	8 Medium	10 High
Rare 1	1 Negligible	2 Negligible	3 Low	4 Low	5 Medium

STAGE 1 - Inherent Risk Rating – Inherent Likelihood Rating X Inherent Impact Rating = Inherent Risk Rating

STAGE 2 – Residual Risk Rating – Residual Likelihood Rating X Residual Impact Rating = Residual Risk Rating

12.4 ANNEXURE 4: THE CITY'S RISK TREATMENT CHART

THE CITY OF MANDURAH RISK TREATMENT CHART					
Risk Level	**Accountability**	**Response**	**Minimum Treatment Required**	**Description**	**Review**
Extreme	Council or CEO	Urgent	Reject and avoid, transfer or mitigate	Immediate action required in consultation with ELT to either avoid the risk entirely, transfer it or to reduce the risk to a low, medium or high rating.	Immediately
High	CEO or ELT	Important	Accept and mitigate	Managers are to be assigned to these risks and treatments to modify, reduce, transfer or eliminate the risk is required.	Monthly
	Treatment Strategies must be applied to risks ≥ High level				
Medium	Executive Manager / Manager or CoMMT	Operational Process	Accept	Manage by specific controls, monitoring or response procedures.	Monthly – Quarterly
Low	Manager / Coordinator / Team Leader	Capture in Risk Register	Accept	Manage by routine procedures.	Quarterly - Annually
Negligible	Manager / Coordinator / Team Leader / Supervisor	Refer to Compliance	Accept	Manage through compliance checks and processes.	Annually

12.5 ANNEXURE 5: ROLES AND RESPONSIBILITIES

THE CITY OF MANDURAH
EVERY PERSON

VISION

A city with a village heart - *where the* ***wellbeing*** *of our* ***people*** *and our* ***environment*** *are nurtured; where* ***business*** *in the* ***community*** *can thrive and entrepreneurship is celebrated*

RISK ROLE & RESPONSIBILITY

Every person is responsible for risk and hazard identification

COUNCIL
ELECTED MEMBERS

STRATEGIC OBJECTIVES

- Community Strategic Plan
- Corporate Business Plan
- Adopted Annual Budgets
- Asset Management Plan
- Long Term Financial Plan
- Workforce Plan

RISK ROLE & RESPONSIBILITY

- Approve Risk Appetite for each strategic objective
- Adopt a Risk Management Policy
- Note the Risk Management Framework
- Note the Management of Strategic Risks
- Establish and maintain an Audit & Risk Committee
- Be kept informed on Risk Management Processes

AUDIT & RISK COMMITTEE

AUDIT OBJECTIVES

- Assurance
- Support
- Compliance

RISK ROLE & RESPONSIBILITY

Make recommendations to Council on:

- Risk Appetite for each strategic objective
- Risk Tools
- How risks are monitored
- Strategic Risk Register
- ≥ High Operational Risks
- Review Risk Treatments & Controls

CEO

STRATEGIC OBJECTIVES

- Community Strategic Plan
- Corporate Business Plan
- Adopted Annual Budgets
- Asset Management Plan
- Long Term Financial Plan
- Workforce Plan

RISK ROLE & RESPONSIBILITY

- Approve & drive implementation of Risk Culture
- Approve the Risk Appetite for each strategic obejective
- Implement the Risk Management Policy
- Implement the Risk Management Framework
- Approve & review management of Strategic Risks
- Approve Business Continuity & Emergency Management Plans
- Oversee ELT's Risk Management responsibilities
- Review the Risk Register
- Ensure resources are allocated to risk management
- Report to Audit & Risk Committee and Council

ELT
DIRECTORS

STRATEGIC OBJECTIVES

- Corporate Business Plan
- Adopted Annual Budgets
- Asset Management Plan
- Long Term Financial Plan
- Workforce Plan

RISK ROLE & RESPONSIBILITY

- Consult on Risk Culture & Risk Appetite on strategic objectives
- Identify, assess and manage Strategic Risks
- Approve Risk Tools
- Approve & review Business Continuity & Emergency Management Plans

In each Directorate:

- Drive implementation of the Risk Management Policy, Framework, Risk Culture & Risk Appetite across Business Areas
- Ensure risk is considered in decision making processes
- Ensure resources are allocated to manage risk
- Own & manage the Directorate's Risk Profile
- Oversee CoMMT Risk Management responsibilities
- Encourage honest reporting and escalation of risks
- Report to the CEO

12.5 ANNEXURE 5: ROLES AND RESPONSIBILITIES (Cont.)

CoMMT
Executive Managers
Business Managers

OPERATIONAL OBJECTIVES

- Business Area Plans
- Business Area Annual Budget

RISK ROLE & RESPONSIBILITY

- Consult on Risk Culture and Strategic Risk Appetite
- Consult on Strategic Risk identification, assessment, treatment & controls
- Consult on Risk Tools
- Prepare Business Continuity & Emergency Management Plans

In each Business Area:

- Drive implementation of the Risk Management Framework and Risk Culture across Teams
- Identify, assess & manage Operational Risks for each Team's projects & tasks
- Ensure risk treatment & controls are current, compliant and within the Strategic Risk Appetite thresholds
- Monitor & review Operational risks in the Business area
- Highlight new and emerging risks
- Recommend suitable Team plans for risk management
- Ensure risk is considered in decision making processes
- Ensure training and resources are allocated to manage risk within each Team
- Encourage honest reporting and escalation of risks
- Report to ELT

TEAM MEMBERS

OPERATIONAL OBJECTIVES

- Team Work & Project Plans

RISK ROLE & RESPONSIBILITY

- Manage risk within their area of responsibility.
- Be informed on Council's Risk Management Policy, Framework & Processes
- Consult on Risk Assessments, Risk Treatments & Action Plans within each Team
- Apply Risk Management processes
- Highlight emerging risks & issues
- Participate & encourage open discussions around risk
- Keep records of risk management tasks
- Participate in Risk Management Training
- Provide Feedback on risk management processes & control effectiveness
- Report to Team Leader/ Business Area Manager

GOVERNANCE
GCR Officer

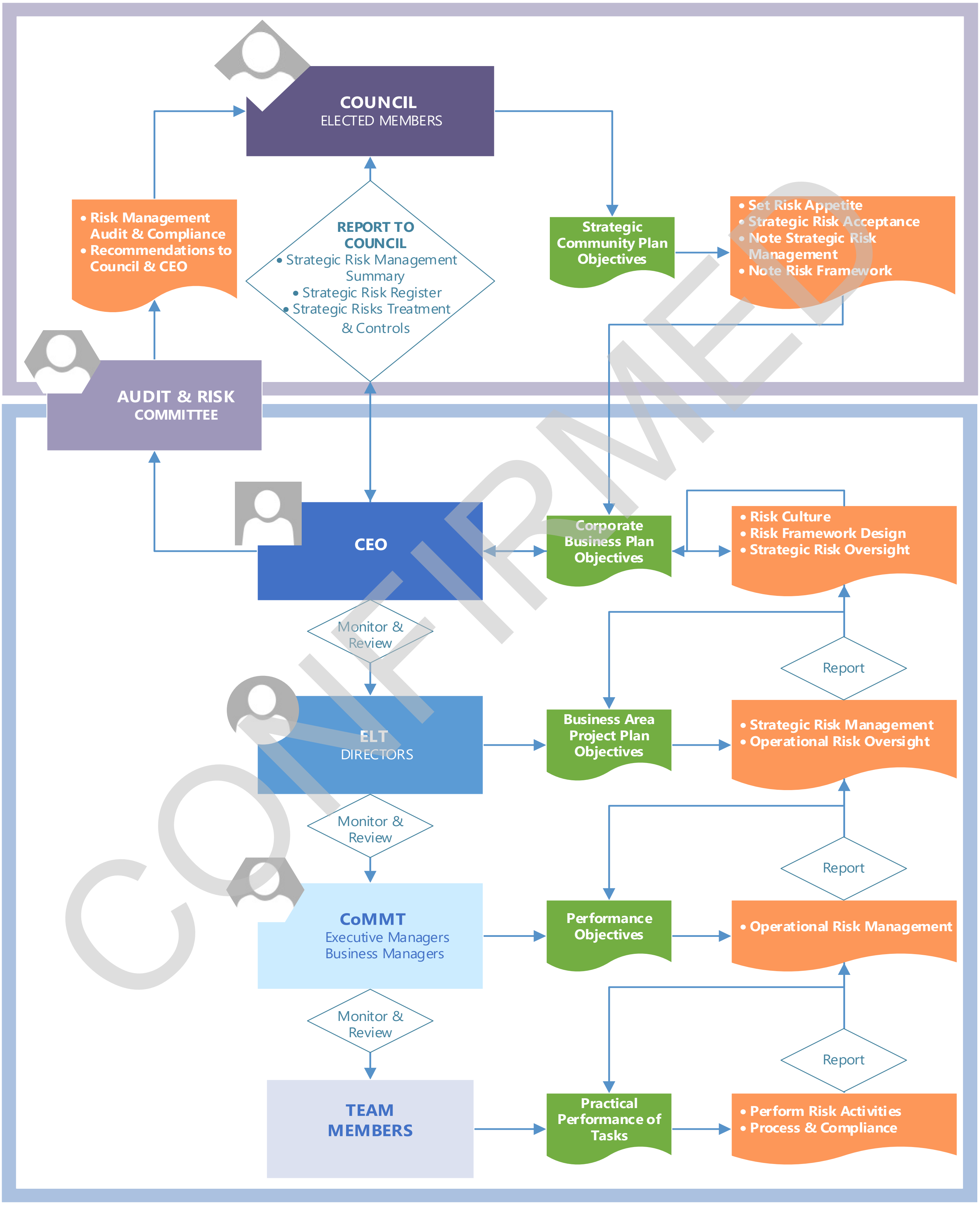
RISK MANAGEMENT OBJECTIVES

- Council Risk Management Policy
- Risk Management Framework

RISK ROLE & RESPONSIBILITY

- Consult on Risk Culture and Strategic Risk Appetite
- Design the Risk Management Framework and procedures & drive effective delivery across the organisation
- Prepare Risk Tools
- Administer Risk Management software
- Consult on Business Continuity & Emergency Management Plans
- Facilitate risk management support and training to all areas across the Organisation
- Undertake assurance audits of the risk management system compliance & effectiveness
- Escalate issues of risk framework non-compliance, risk mismanagement & high emerging risks to the CEO
- Report to Governance and Director Corporate Services

12.6 ANNEXURE 6: OVERVIEW OF THE RISK MANAGEMENT FRAMEWORK



COUNCIL
ELECTED MEMBERS

- Risk Management Audit & Compliance
- Recommendations to Council & CEO

REPORT TO COUNCIL

- Strategic Risk Management Summary
- Strategic Risk Register
- Strategic Risks Treatment & Controls

Strategic Community Plan Objectives

- Set Risk Appetite
- Strategic Risk Acceptance
- Note Strategic Risk Management
- Note Risk Framework

AUDIT & RISK COMMITTEE

CEO

Corporate Business Plan Objectives

- Risk Culture
- Risk Framework Design
- Strategic Risk Oversight

Monitor & Review

Report

ELT
DIRECTORS

Business Area Project Plan Objectives

- Strategic Risk Management
- Operational Risk Oversight

Monitor & Review

Report

CoMMT
Executive Managers
Business Managers

Performance Objectives

- Operational Risk Management

Monitor & Review

Report

TEAM MEMBERS

Practical Performance of Tasks

- Perform Risk Activities
- Process & Compliance

12.7 ANNEXURE 7: RISK MANAGEMENT TERMS AND DEFINITIONS

Definitions of terms used have been sourced from Australian ISO Standard on Risk Management: AS ISO 31000:2018

TERMS	DEFINITIONS AND EXPLANATIONS
Consequence	Outcome of an event affecting objectives – also expressed as **impact** or **severity.**
Control	Measure that maintains and / or modifies risk. Controls may be directive, preventative, detective, corrective or any other mitigating action to minimise the impact of an identified risk.
Event	Occurrence or change of a particular set of circumstances – also expressed as **incident.**
Impact	The outcome of an event expressed either in financial terms or qualitatively, being a loss, injury, disadvantage or gain.
Inherent Risk	The raw risk present without considering controls, mitigating factors or treatment applied to it.
Likelihood	Chance of something happening – also expressed as **probability.**
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
Operational Risk	Risk associated with The City's core operational / business functions and: • may impact on the directorate, business unit or service unit achieving its unit plan objectives; • may impact delivery of specific City services and programs; • is managed by CoMMT.
Project Risk	Risk associated with a City project and: • may affect the milestones connected with the delivery of the project on time, within budget or within agreed acceptable quality parameters; • is identified at all stages of the project, discreet activities or program lifecycle; • is managed with operational risks by a designated Project Manager and an assigned Directorate.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
Risk	Effect of uncertainty on objectives. It is measured in terms of likelihood of an event and its impact.

TERMS	DEFINITIONS AND EXPLANATIONS
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk, by defining its likelihood and consequence.
Risk Appetite	The level of risk that Council is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Criteria	Terms of reference by which risk is assessed - organisational objectives, risk appetite, external and internal context, standards, laws, policies and other requirements.
Risk Evaluation	Process of comparing the risk level with risk criteria to determine whether or not the level of risk is acceptable.
Risk Identification	Process of finding, recognising and describing risk.
Risk Level	Magnitude of a risk calculated by multiplying the risk's level of likelihood by its level of impact.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Profile	The residual risk impact and likelihoods reflected on a heat map to illustrate The City's risk exposure at a glance.
Risk Register	Risk management tool to record details for identified risk, including risk ratings, nature of the risk, owner, manager, and mitigation measures.
Risk Source	Element which alone or in combination has the potential to give rise to risk.
Risk Treatment / Action Plan	The additional controls / mitigation action required to ensure that the risk appetite level is achieved.
Residual Risk	The risk level remaining after taking account of the effectiveness of controls and mitigating actions.
Stakeholder	Person or organisation that can affect, be affected by, or perceive to be affected by a decision or activity.