

NOTICE OF MEETING

AUDIT AND RISK COMMITTEE

Members of the Audit and Risk Committee are advised that a meeting of the Committee will be held in the Council Chambers, Civic Building, 83 Mandurah Terrace, Mandurah and via eMeeting on:

**Tuesday 8 September 2020
at 5.30pm**

MARK R NEWMAN

Chief Executive Officer
1 September 2020

Committee Members:

Councillor P Jackson (Chairperson)
Mayor Williams
Councillor J Green
Councillor P Rogers
Councillor A Zilani
Mr W Ticehurst

Deputies:

Councillor D Lee
Councillor D Pember

AGENDA

1 OPENING OF MEETING

2 APOLOGIES

3 IMPORTANT NOTE

Members of the public are advised that the decisions of this Committee are referred to Council Meetings for consideration and cannot be implemented until approval by Council. Therefore, members of the public should not rely on any decisions of this Committee until Council has formally considered the resolutions agreed at this meeting.

4 RESPONSE TO PREVIOUS QUESTIONS TAKEN ON NOTICE

5 PUBLIC QUESTION TIME

Public Question Time provides an opportunity for members of the public to ask a question of Council. For more information regarding Public Question Time please visit the City's website www.mandurah.wa.gov.au or telephone 9550 3787.

6 ANNOUNCEMENTS

Modification to *Standing Orders Local Law 2016* - electronic attendance at meeting.

7 PRESENTATIONS

Occupational Safety and Health Annual Review 2019-2020

Strategic Risk Management Update

8 DEPUTATIONS

Any person or group wishing to make a Deputation to the Committee meeting regarding a matter listed on this agenda for consideration must complete an application form. For more information regarding making a deputation please visit the City's website www.mandurah.wa.gov.au or telephone 9550 3787.

NB: Persons making a deputation to this Committee meeting will not be permitted to make a further deputation on the same matter at the successive Council meeting, unless it is demonstrated there is new, relevant material which may impact upon the Council's understanding of the facts of the matter.

9 CONFIRMATION OF MINUTES: 16 JUNE 2020 (Attached)**10 DECLARATIONS OF INTERESTS****11 QUESTIONS FROM COMMITTEE MEMBERS**

11.1 Questions of Which Due Notice Has Been Given

11.2 Questions of Which Notice Has Not Been Given

12 BUSINESS LEFT OVER FROM PREVIOUS MEETING**13 REPORTS FROM OFFICERS:**

1	Strategic Internal Audit Update and Progress Update on Regulation 17 Review (BS)	1 - 8
2	Office of the Auditor General – Local Government Systems Performance Audit (BS)	9 - 18
3	Office of the Auditor General: Regulation of Consumer Food Safety by Local Government Entities (BS)	19 - 26
4	Office of the Auditor General: Working with Children Checks - Managing Compliance (S&ED)	27 - 30
5	Occupational Safety and Health (OSH) 2019-2020 Annual Review (S&ED)	31 - 44
6	2020 Local Government Insurance Services 3 Steps to Safety Program (S&ED)	45 - 68

14 LATE AND URGENT BUSINESS ITEMS**15 CLOSE OF MEETING**



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

Councillor Schumacher (Non-Committee)

Apologies

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)**

Summary

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

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;

RISK MANAGEMENT

- 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**.

RISK MANAGEMENT

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

Risk Management Framework

Table of contents

1.	Introduction.....	17
2.	Objective.....	17
3.	Legislative Context	17
4.	Australian Standard on Risk Management – AS ISO 31000:2018.....	19
5.	Risk Management Principles.....	20
6.	Council's Risk Management Policy (POL-RKM 01)	21
7.	Risk Management Assurance	22
8.	Risk Appetite	25
9.	Strategic and Operational Risk Management.....	26
10.	Risk Management Process	27
11.	Roles and Responsibilities.....	43
12.	Annexures	44

Risk Management Framework

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

Risk Management Framework

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

Risk Management Framework

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:

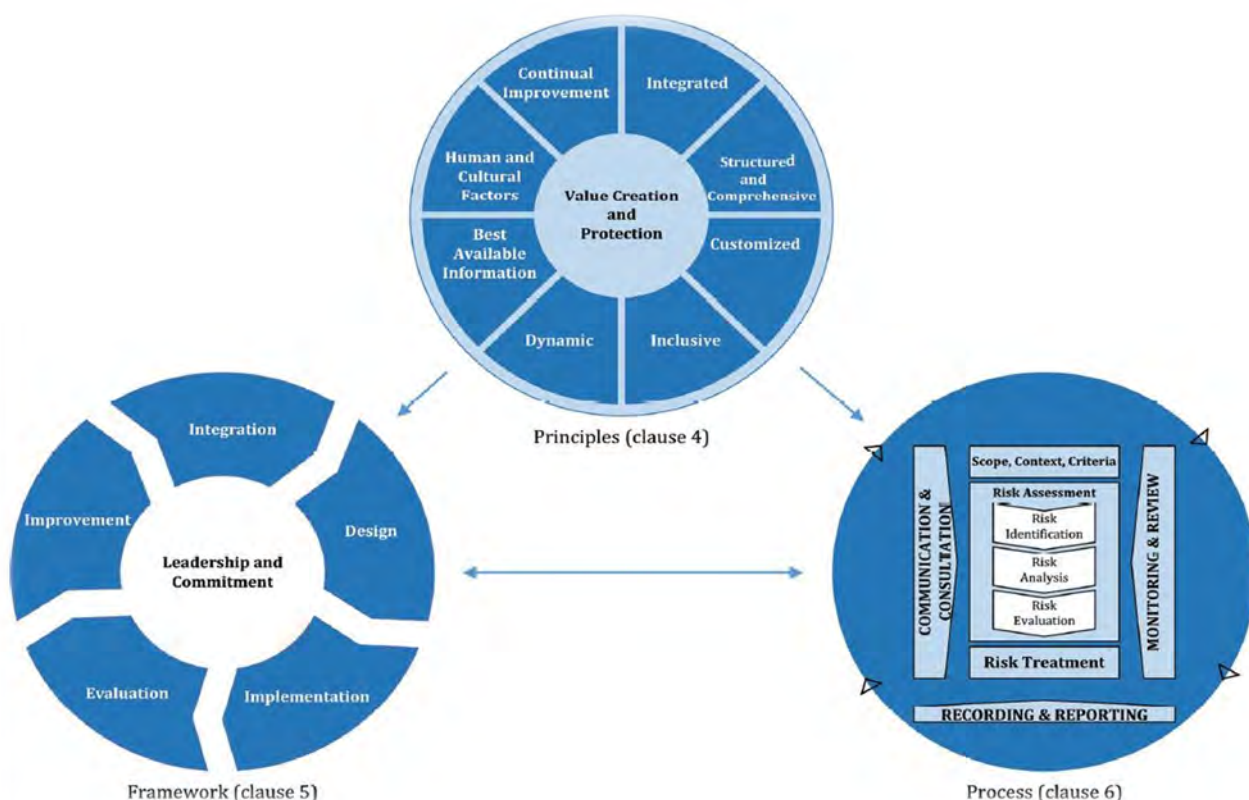


Figure 1 –AS ISO 31000:2018 recommended Risk Management System

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.

Risk Management Framework

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**.



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

Risk Management Framework

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.

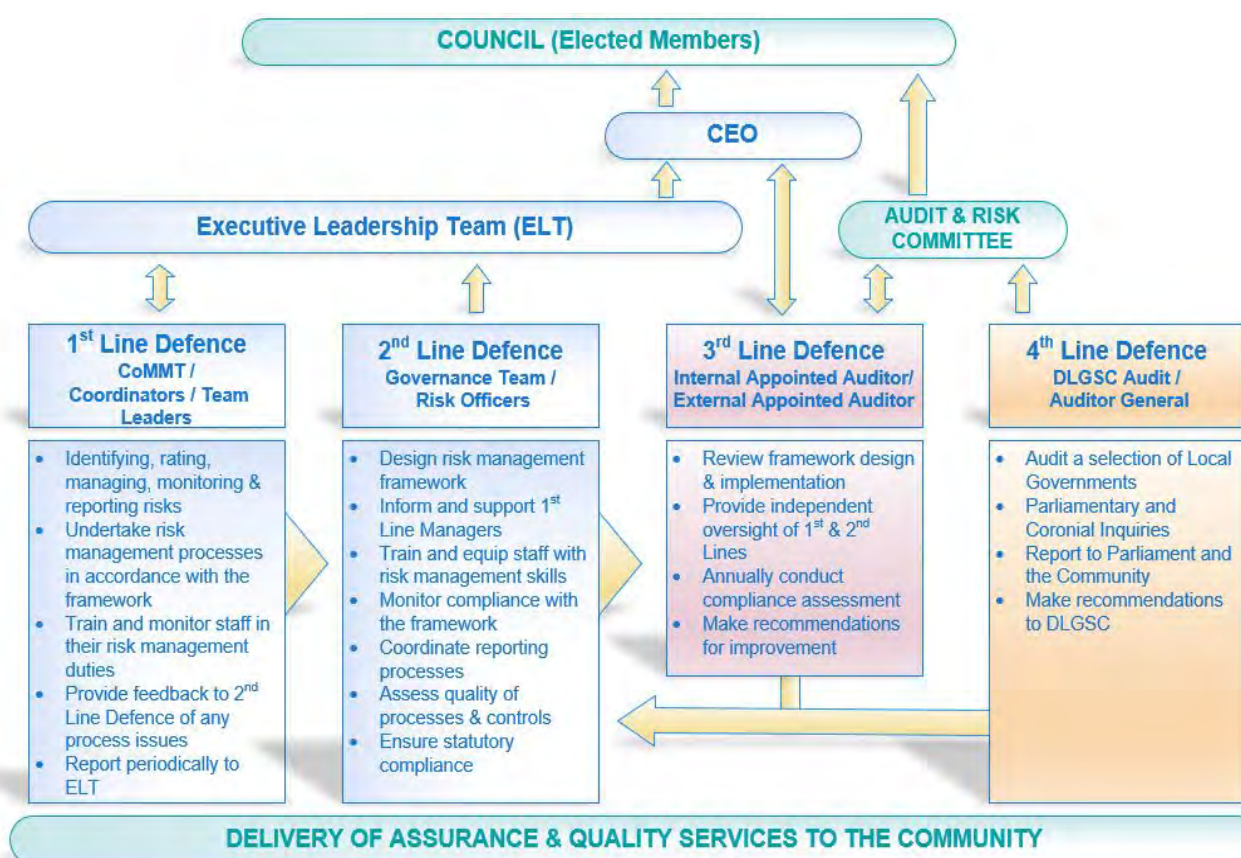
⁹ City of Mandurah (2020) *Risk Management Policy*, Council Policy POL-RKM01.

Risk Management Framework

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.



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.

Risk Management Framework

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.

Risk Management Framework

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.

Risk Management Framework

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.

Risk Management Framework

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.

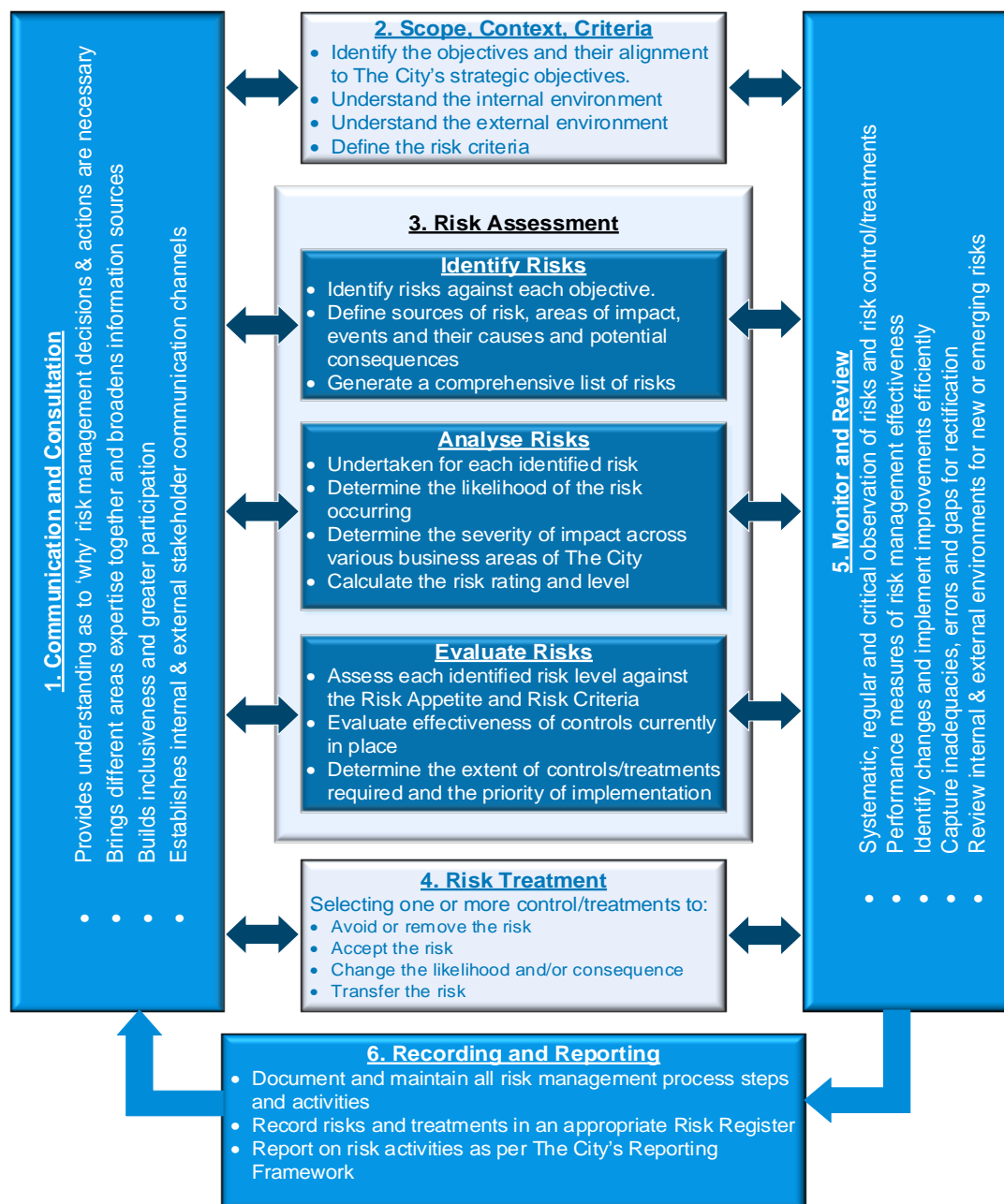
Operational risks also include Project Risks. Project risks are risks associated with individual projects, initiatives or day-to-day business activities at the City. Project risks are to be assessed in the project planning phase and throughout the duration of the project's business activities.

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

Risk Management Framework

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 Standard¹¹ with the following commentary providing broad descriptions of each step:



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

Risk Management Framework

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.

Risk Management Framework

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.

Risk Management Framework

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 Management Framework

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***.

$$\text{Risk Likelihood} \quad \times \quad \text{Risk Impact} \quad = \quad \text{Risk Rating}$$

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.

Risk Management Framework

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 table¹⁵ 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.

Risk Management Framework

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.

Risk Management Framework

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

Residual Risk Level:

THE CITY OF MANDURAH RISK RATING CHART						
	Likelihood Rating	X	Impact Rating	=	Risk Rating	
	Insignificant 1		Minor 2		Major 4	Catastrophic 5
Almost Certain 5	5 Medium		10 High		20 Extreme	25 Extreme
Likely 4	4 Low		8 Medium		16 High	20 Extreme
Possible 3	3 Low		6 Medium		12 High	15 High
Unlikely 2	2 Negligible		4 Low		8 Medium	10 High
Rare 1	1 Negligible		2 Negligible		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.

Risk Management Framework

		• 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
<ul style="list-style-type: none"> More treatment is urgently required 	Decided on a case by case basis – <ul style="list-style-type: none"> more treatment required; or accept with ELT strict & regular monitoring 	Decided on a case by case basis – <ul style="list-style-type: none"> accept & monitor; or more treatment required 	<ul style="list-style-type: none"> Accept & monitor – no further treatment required 	<ul style="list-style-type: none"> 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.

Risk Management Framework

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 OPTIONS¹⁹

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.

Risk Management Framework

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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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?

Risk Management Framework

- 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

Risk Management Framework

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 <u>little</u> scope for improvement.	Processes (Controls) operating as intended and aligned to Policies / Procedures. Subject to ongoing monitoring. Reviewed and tested regularly.
Adequate	There is <u>some</u> scope for improvement.	Processes (Controls) generally operating as intended, however inadequacies exist. Limited monitoring. Reviewed and tested, but not regularly.
Inadequate	There is a <u>need</u> 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.

Risk Management Framework



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.

Risk Management Framework

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	RECEIPT/ 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.

Risk Management Framework

DOCUMENT NAME	AUTHOR	RECEIPT/ 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.

Risk Management Framework

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 \geq 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.

Risk Management Framework

12. Annexures

ANNEXURE 1: [THE CITY'S RISK LIKELIHOOD RATING TABLE](#)

ANNEXURE 2: [THE CITY'S RISK IMPACT TABLE](#)

ANNEXURE 3: [THE CITY'S RISK RATING CHART](#)

ANNEXURE 4: [THE CITY'S RISK TREATMENT CHART](#)

ANNEXURE 5: [ROLES AND RESPONSIBILITIES](#)

ANNEXURE 6: [OVERVIEW OF THE RISK MANAGEMENT FRAMEWORK](#)

ANNEXURE 7: [RISK MANAGEMENT TERMS AND DEFINITIONS](#)

Risk Management Framework

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.

Risk Management Framework

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

Risk Management Framework

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

Risk Management Framework

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

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






Risk Management Framework

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 \geq 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

Risk Management Framework

12.5 ANNEXURE 5: ROLES AND RESPONSIBILITIES

 <p>THE CITY OF MANDURAH EVERY PERSON</p>	<p>VISION</p>								
 <p>COUNCIL ELECTED MEMBERS</p>	<p>A city with a village heart - where the <i>wellbeing</i> of our <i>people</i> and our <i>environment</i> are nurtured; where <i>business</i> in the <i>community</i> can thrive and entrepreneurship is celebrated</p> <p>RISK ROLE & RESPONSIBILITY</p> <p>Every person is responsible for risk and hazard identification</p>								
 <p>AUDIT & RISK COMMITTEE</p>	<table> <tr> <th data-bbox="550 544 869 611">STRATEGIC OBJECTIVES</th><th data-bbox="869 544 1508 611">RISK ROLE & RESPONSIBILITY</th></tr> <tr> <td data-bbox="550 611 869 801"> <ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan </td><td data-bbox="869 611 1508 801"> <ul style="list-style-type: none"> 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 </td></tr> <tr> <th data-bbox="550 801 869 869">AUDIT OBJECTIVES</th><th data-bbox="869 801 1508 869">RISK ROLE & RESPONSIBILITY</th></tr> <tr> <td data-bbox="550 869 869 936"> <ul style="list-style-type: none"> Assurance Support Compliance </td><td data-bbox="869 869 1508 936"> <p>Make recommendations to Council on:</p> <ul style="list-style-type: none"> Risk Appetite for each strategic objective Risk Tools How risks are monitored Strategic Risk Register ≥ High Operational Risks Review Risk Treatments & Controls </td></tr> </table>	STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY	<ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> 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 OBJECTIVES	RISK ROLE & RESPONSIBILITY	<ul style="list-style-type: none"> Assurance Support Compliance 	<p>Make recommendations to Council on:</p> <ul style="list-style-type: none"> Risk Appetite for each strategic objective Risk Tools How risks are monitored Strategic Risk Register ≥ High Operational Risks Review Risk Treatments & Controls
STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY								
<ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> 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 OBJECTIVES	RISK ROLE & RESPONSIBILITY								
<ul style="list-style-type: none"> Assurance Support Compliance 	<p>Make recommendations to Council on:</p> <ul style="list-style-type: none"> Risk Appetite for each strategic objective Risk Tools How risks are monitored Strategic Risk Register ≥ High Operational Risks Review Risk Treatments & Controls 								
 <p>CEO</p>	<table> <tr> <th data-bbox="550 936 869 1003">STRATEGIC OBJECTIVES</th><th data-bbox="869 936 1508 1003">RISK ROLE & RESPONSIBILITY</th></tr> <tr> <td data-bbox="550 1003 869 1339"> <ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan </td><td data-bbox="869 1003 1508 1462"> <ul style="list-style-type: none"> Approve & drive implementation of Risk Culture Approve the Risk Appetite for each strategic objective 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 </td></tr> </table>	STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY	<ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> Approve & drive implementation of Risk Culture Approve the Risk Appetite for each strategic objective 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 				
STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY								
<ul style="list-style-type: none"> Community Strategic Plan Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> Approve & drive implementation of Risk Culture Approve the Risk Appetite for each strategic objective 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 								
 <p>ELT DIRECTORS</p>	<table> <tr> <th data-bbox="550 1216 869 1283">STRATEGIC OBJECTIVES</th><th data-bbox="869 1216 1508 1283">RISK ROLE & RESPONSIBILITY</th></tr> <tr> <td data-bbox="550 1283 869 1686"> <ul style="list-style-type: none"> Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan </td><td data-bbox="869 1283 1508 2007"> <ul style="list-style-type: none"> 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 <p><u>In each Directorate:</u></p> <ul style="list-style-type: none"> 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 </td></tr> </table>	STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY	<ul style="list-style-type: none"> Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> 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 <p><u>In each Directorate:</u></p> <ul style="list-style-type: none"> 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 				
STRATEGIC OBJECTIVES	RISK ROLE & RESPONSIBILITY								
<ul style="list-style-type: none"> Corporate Business Plan Adopted Annual Budgets Asset Management Plan Long Term Financial Plan Workforce Plan 	<ul style="list-style-type: none"> 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 <p><u>In each Directorate:</u></p> <ul style="list-style-type: none"> 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 								

Risk Management Framework

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

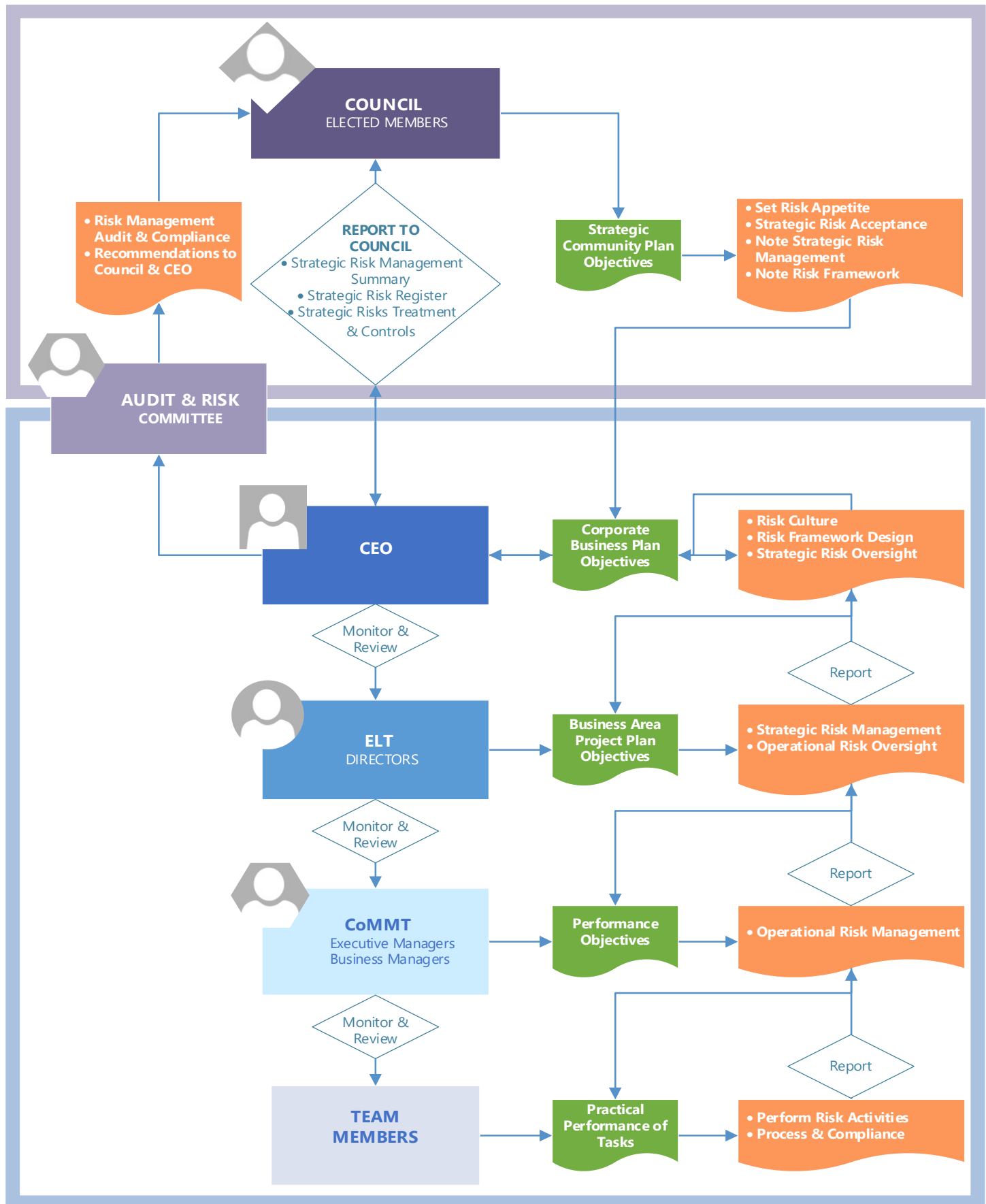
- Council Risk Management Policy
- Risk Management Framework

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

Risk Management Framework

12.6 ANNEXURE 6: OVERVIEW OF THE RISK MANAGEMENT FRAMEWORK



Risk Management Framework

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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.

Risk Management Framework

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.

01 **SUBJECT:** Strategic Internal Audit Update and Progress Update on Regulation 17 Review
 DIRECTOR: Director Business Services
 MEETING: Audit and Risk Committee
 MEETING DATE: 8 September 2020

Summary

The City of Mandurah (the City) Strategic Internal Audit function was adopted by Council on 26 May 2020 and the function was formally implemented on 1 July 2020. In accordance with the Internal Audit Plan, the Audit and Risk Committee is required to receive a Strategic Internal Audit Plan Monitoring Report on a quarterly basis, with the first report due to the Audit and Risk Committee at the meeting of 1 December 2020. This report will set out the internal audit findings for any audits conducted in quarter one and two, including any recommendations, the City's actions and a progress update.

In April 2020, the Chief Executive Officer (CEO) engaged an external audit service provider to conduct a review of risk management, internal controls and legislative compliance, in accordance with Regulation 17(1) of the *Local Government (Audit) Regulations 1996* (Regulations). This review, required every three years determines the appropriateness and effectiveness of the City's systems and procedures in relation to risk management, internal controls and legislative compliance. The Audit and Risk Committee received the report at its meeting on 19 May 2020 and noted a number of recommendations for improvement.

Whilst this internal audit was undertaken prior to the implementation of the City's formal internal audit function, the progress on the implementation of the recommendations are to be monitored in accordance with the Internal Audit Plan.

A progress update (**Confidential Attachment 1.1**) is now being presented to the Audit and Risk Committee for review and noting prior to being presented to Council.

Disclosure of Interest

Nil

Previous Relevant Documentation

- | | | |
|--------------|------------------|---|
| • G.13/5/20 | 26 May 2020 | CEO Review of Risk Management, Internal Controls & Compliance |
| • G.12/5/20 | 26 May 2020 | Strategic Internal Audit Plan 2020/21- 2022/23 |
| • G.26/5/17 | 8 May 2017 | Risk Management, Internal Controls & Legislative Compliance - CEO Biennial Report |
| • G.12/11/14 | 25 November 2014 | Review of Internal Controls: Risk Management |
| • G.8/11/18 | November 2018 | Part Implementation of Internal Audit Function |
| • AR.7/5/17 | May 2017 | Internal Audit Function: Proposed Approach |
| • G.20/5/16 | May 2016 | Implementation of an Internal Audit Function |
| • G.11/11/14 | November 2014 | Development of an Internal Audit Function |
| • G.17/7/14 | July 2014 | Role of Internal Audit |

Background

At the Audit and Risk Committee on 19 May 2020, the Committee reviewed the City's Strategic Internal Audit Plan 2020/21 -2022/23, Internal Audit Charter, Internal Audit Plan and amendments to the Audit and Risk Committee Terms of Reference before the documents are presented to Council for adoption. The Internal Audit Plan was adopted by Council on 26 May 2020 and formally implemented on 1 July 2020.

The Regulation 17 review was undertaken by an external audit service provider in April 2020 and the review was noted by Council on 26 May 2020. The review identified a number of recommendations for improvements that are required to be progressed over a 12 – 18 month period.

Comment

Strategic Internal Audit Plan

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

In addition to supporting good internal governance and ongoing improvements to the City's operations, internal audit should also help to instil public confidence in the City's ability to operate effectively.

The purpose of the City's internal audit function is to:

- Provide independent, objective assurance and consulting services designed to add value and improve the City's operations;
- Enhance and protect organisational value by providing risk-based and objective assurance, advice and insight; and
- Help the City accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

Underpinning the SIAP is an Operational Internal Audit Plan 2020/21 (OIAP) setting out the audit activity, detailed scope and resourcing requirements for the first year of the SIAP. There are six internal audits planned to be delivered in accordance with the OIAP 2020/2021. Below is a status update on the planned audits:

Audit Ref	Internal Audit Area	Objective	Update	2020/2021			
				Q1	Q2	Q3	Q4
2020.21_ IA1	Procurement	<ol style="list-style-type: none"> 1. Evaluate the effectiveness of the Procurement Policy, procedures and practises 2. Ensure compliance with the statutory obligations for tenders and tender exempt 3. Support ongoing improvement 4. Inform education and training programs. 	This is not scheduled to commence until January to March 2021			✓	
2020.21_ IA2	Crisis Governance and Response	<ol style="list-style-type: none"> 1. Evaluate the effectiveness of the City's governance, systems, controls and response to the COVID-19 Pandemic. 2. Support the development, improvement and readiness for future crisis governance and response. 	It is proposed to defer the commencement of this audit until quarter three (January to March 2021). This will provide further time to assess whether there is a 'second wave' in Western			✓	

		3. Inform education and training programs relating to crisis governance.	Australia and if so, the City's response				
2020.21_ IA3	Compliance Audit Return	1. Assess the overall effectiveness of the City's compliance with the requirements of the Act and its Regulations. 2. Support ongoing improvement 3. Inform education and training programs.	Internal audit tool and procedure developed. Commencing audit in September (in house).			✓	
2020.21_ IA4	Financial Management Systems and Procedures	1. To review the appropriateness and effectiveness of the financial management systems and procedures. 2. Support ongoing improvement 3. Inform education and training programs.	Quotes obtained. Commencing audit in December 2020.			✓	
2020.21_ IA5	Information Technology	1. Determine the need for improved security controls. 2. Reduce risk for the City. 3. Inform education and training programs.	A request for quote to be issued in late September.		✓		
2020.21_ IA6	Occupational Safety and Health (progress review)	1. To evaluate the safety and health management systems. 2. Monitor progress and implementation of improvements from previous audit. 3. Reduce risk for the City. 4. Inform education and training programs	The full audit has significantly progressed. This audit is a progress review of the 2019/20 audit and test the City's progress towards implementation of recommendations.				✓

The Audit and Risk Committee will receive a SIAP Monitoring Report on a quarterly basis, with the first report due to the Audit and Risk Committee on 1 December 2020. This report will set out the internal audit findings on audits conducted during quarter one and quarter two, including any recommendations, City's actions and progress update.

Regulation 17 Review Progress Update

An independent internal audit service provider was appointed by the CEO to undertake the regulation 17 Review in April 2020. The findings from the review represent an opportunity for continuous improvement to the City's governance, compliance and risk systems.

Since the last report to the Audit and Risk Committee in May 2020, the City has progressed the implementation of the recommendations, refer to *Confidential Attachment 1.1*. Regular updates will be provided to the Audit and Risk Committee on the implementation of the findings over the next 12 – 18 months.

Consultation

Consultation is undertaken with business areas prior to internal audits being undertaken.

Policy Implications

Relevant CEO Policies and Council Policies.

Economic Implications

It is envisaged that six programmed audits would be conducted each year. An approximate cost of \$150,000 per annum can be anticipated for the service. This amount is budgeted for in the 2020/21 financial year.

Risk Analysis

Internal audit is an essential part of an organisation's risk management strategy. The function both reports on financial, compliance and operational controls as well as adding value to an organisation through identifying areas of improvement in systems and processes.

Strategic Implications

The following strategies from the *City of Mandurah Strategic Community Plan 2020 – 2040* are relevant to this report:

Organisational Excellence:

- Build and retain a skilled, agile, motivated and healthy workforce.
- Ensure the City has the capacity and capability to deliver quality services and facilities through accountable and transparent business practices, governance, risk and financial management.

Conclusion

The regulation 17 review presented an opportunity to implement improvements to the City's risk management, internal controls and legislative compliance. Significant progress has been made in recent months on the implementation of improvements identified as part of this review. The Audit and Risk Committee are recommended to not the progress update on the improvements identified. The City will continue to progress the improvements over the next 12 to 18 months and regular reporting will be provided to Audit and Risk Committee on the progress.

NOTE:

- Refer ***Confidential Attachment 1.1*** ***Progress update on Regulation 17 Review***

RECOMMENDATION

That the Audit and Risk Committee note the progress update on the implementation of the improvements from the review of risk management, internal controls and legislative compliance as per Confidential Attachment 1.1.

02	SUBJECT:	Office of the Auditor General – Local Government Systems Performance Audit
	DIRECTOR:	Director Business Services
	MEETING:	Audit and Risk Committee
	MEETING DATE:	8 September 2020

Summary

The Auditor General has issued a performance audit report assessing the general information technology (IT) controls at 10 local governments. Each entity was assessed over fourteen categories. The City of Mandurah was not one of the 10 local governments included in the Auditor General audit.

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 performance audit.

Disclosure of Interest

Nil

Previous Relevant Documentation

- G.10/6/20 23 June 2020 A comparison of the City's systems with the Auditor General's report on State Government entities.

Background

The Office of the Auditor General (OAG)¹ has carried out its first performance audit on the effectiveness of information systems in local government. A total of 10 local governments were evaluated in a security gap analysis against the fourteen areas of the ISO 27002 standard. These are:

Information security aspects of business continuity management	Physical and environmental security
Human resources security	Information security policies
Access control	System acquisition, development and maintenance
Communications security	Operations security
Information security incident management	Compliance
Organisation of information security	Supplier relationships
Asset management	Cryptography

In addition, there was also an assessment of general computer controls including:

- Local governments had identified and defined the security requirements based on the risks to their information systems.
- Appropriate controls were in place to mitigate information security risks.
- Mitigating controls were in place where practices did not align with international standards.

¹ Due to the size of the Auditor General's report it has not been included as an attachment. The report can be accessed at <https://audit.wa.gov.au/reports-and-publications/reports/information-systems-audit-report-2020-lg/>

For this part of the report each category was assigned a score based on the following table:

0 Non-existent	Management processes are not applied at all. Complete lack of any recognisable processes.
1 Initial/ad hoc	Processes are ad hoc and overall approach to management is disorganised.
2 Repeatable but intuitive	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 Defined	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated; however it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 Managed and measurable	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimised	Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the entity quick to adapt.

The general finding was that:

“All of the audited entities had significant gaps in meeting the good practice standard across several control areas (Figure 2). Only 4 entities demonstrated that they were effective, or partially effective in at least 7 of the 14 areas. In order to protect the security of the information and systems of the audited entities, we have not named them in this report. We provided each audited entity with a copy of their gap analysis results.”

Comment

Comments regarding the City’s position compared to the control weaknesses are included in Confidential Attachment 2.1.

In addition, the following points are noted:

- The OAG’s report has generated a significant amount of discussion between IT managers across local government. The OAG expressed the view that:

“We found that all 10 local government entities had significant shortcomings in their information security practices. Entities need to seriously consider these standards and the recommendations in this report to improve information security practices and protect the confidentiality, integrity and availability of information and systems.”

“International standards provide a good framework and starting point for entities to develop and implement sound practices in their operational and strategic security processes. My Office will continue to monitor and report on general computer controls and capability assessments of local government entities. We expect to see better results similar to the improvements made in the State sector in recent years as reported through our regular information system audit program.”

The local government sector has raised concerns that local governments do not have the resources to be able to emulate better provisioned agencies such as State Government entities. Comments have been made to WA Local Government Association (WALGA) that a meeting be held with the OAG to discuss the differences and constraints placed upon local government.

This approach is not supported by City Officers. The intention of the OAG when carrying out performance audits is not to use reports to portray entities in a bad light. Rather, it is to provide the guidance and direction on how improvements can be made. The OAG's report needs to be viewed in a positive way as providing a roadmap for improvement.

- There is no doubt that, on occasions, the availability of resources will constrain the ability to implement a particular improvement. This occurs frequently in many organisations, both public and private. In most cases, these issues can be overcome by planning activities over a longer period than the current budget cycle. The use of risk analysis can help in understanding the priorities within planning.
- 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. This report is more detailed and covers more areas than what the OAG provided for their audit of IT systems controls in State Government entities. Despite that, the comparison is a useful exercise, and is largely favourable with improvements required in risk management and disaster recovery testing.

Consultation

Nil

Statutory Environment

Section 5.41(h) of the *Local Government Act 1995*. Functions of CEO

"ensure that records and documents of the local government are properly kept for the purposes of this Act and any other written law"

Policy Implications

Nil

Economic Implications

Nil

Risk Analysis

The inability to maintain systems which are as robust as possible presents risks both in terms of data loss and impairment of operating capability. Damage would then be seen to the City's reputation and possibly to stakeholders such as suppliers and the community.

Strategic Implications

The following strategy from the *City of Mandurah Strategic Community Plan 2020 – 2040* is relevant to this report:

Organisational Excellence:

- Ensure the City has the capacity and capability to deliver quality services and facilities through accountable and transparent business practices, governance, risk and financial management.

Conclusion

The OAG's report on the audit of system controls in local government provides a very useful roadmap to assist with the improvement of the City's systems.

It is recommended that the Audit and Risk Committee note the City officers comments outlined in Confidential Attachment 2.1.

NOTE:

- Refer ***Confidential Attachment 2.1 Comparison of City systems with Auditor General's report on local government.***

RECOMMENDATION

That the Audit and Risk Committee note the comparison of the status of the City's general computer controls with the findings of the Auditor General's report on Local Government as detailed in Confidential Attachment 2.1.

03	SUBJECT:	Office of the Auditor General: Regulation of Consumer Food Safety by Local Government Entities
	DIRECTOR:	Director Business Services
	MEETING:	Audit & Risk Committee
	MEETING DATE:	8 September 2020

Summary

The Office of the Auditor General (OAG)¹ has released a report on the Regulation of Consumer Food Safety by Local Government Entities that was tabled on 30 June 2020. The OAG selected a sample of two local government entities to conduct the audit. These two local governments were selected because they have a large number of food businesses such as restaurants, cafes and bars.

The original scope of the performance audit included the Department of Health (DoH) however due to the impact of COVID-19, the DoH will be subject to a separate audit at a later date.

Disclosure of Interest

Nil

Previous Relevant Documentation

N/A

Background

The OAG routinely conduct audits of matters considered to be risk areas called performance audits. This audit focused on the regulation of consumer food safety by local government entities and outlined five recommendations that local government entities should consider.

It is expected that all local governments should review their current procedures and implement any necessary changes to align with the findings of the report. The City has undertaken such a review and provides the following feedback.

Comment

All local governments have an essential role to ensure food business proprietors understand their legal responsibilities to comply with the *Food Act 2008* (Act), *Food Regulations 2009* and the Australia New Zealand Food Standards (Code).

Local governments should have an effective food safety education, enforcement and compliance program in place to assess compliance with the relevant requirements and take the necessary enforcement action where required.

Food safety activities within the City of Mandurah are undertaken in the following areas:

- Approvals of permanent and temporary food operations;
- Routine surveillance and assessments including inspection and sampling of food businesses;
- Response activities including complaint, food poisoning outbreak investigation and food recall actioning;
- Training and promotion.

¹ Due to the size of the Auditor General's report it has not been included as an attachment. The report can be accessed at <https://audit.wa.gov.au/reports-and-publications/reports/regulation-of-consumer-food-safety-by-local-government-entities/>

The aim of the OAG audit was to assess whether local government entities effectively regulate consumer food safety in food businesses located within their jurisdiction. The report focused on the following inspection and enforcement processes:

- Food business risk classification;
- Inspection frequency;
- Record management;
- Non-compliance enforcement and follow-up.

The City currently has 562 food businesses registered under the Act. The recent City of Mandurah regulation 17 (internal controls, risk and compliance) *Local Government (Audit) Regulations 1996* audit included some similar elements of the audit completed by the OAG with a particular focus on the current food business register. From the regulation 17 audit, there were no recommendations made about the City's management of the food business register.

It is encouraging that the OAG mentioned the importance of educating businesses on appropriate safe food handling practices as being part of the overall regulatory regime. Food handler skills and knowledge are an essential component of the sale of safe food and positive food safety culture which has been an important focus for the City of Mandurah for some time.

As part of its audit of the two local governments, the OAG found that *'many inspections were overdue, recordkeeping was poor, and follow-up and enforcement was not always completed or consistent'*. It was highlighted that it is not the intention of the report to increase regulation, however a fair and equitable regulatory framework should be in place that focuses on areas of greatest risk to the community.

The City Officers have commented on the City's current practices to the OAG audit findings and the findings are detailed in Confidential Attachment 3.1.

As mentioned in the report, it is vital that food handlers and food business proprietors have the appropriate skills and knowledge to prepare and sell safe food to the community. In order to support food businesses with training their employees the City offers the following:

- FoodSafe
 - FoodSafe is a training package aimed at food business proprietors and provides effective tools to train their employees in safe food handling practices and includes documented templates to ensure effective records are kept. There is also an on-line introduction to food safety course aimed at all food handlers which the City pays a subscription fee and offers food businesses free access through the City's website.
- On-site food handler training
 - City Officers deliver food safety presentations on-site at the request of food businesses or as recommended by officers if there are concerns about skills and knowledge of food handlers.
- Food safety email notifications
 - Email notifications are routinely sent to food business and topics are chosen based on common non-compliances observed by officers during assessments, state/nationwide food safety concerns (ie safe handling of eggs) and other community issues.

Consultation

In August 2019, the City undertook a food business survey to assess feedback on the performance of Environmental Health Officers in completing their duties with the following feedback provided:

	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE	TOTAL
The Environmental Health Officer was polite and respectful	76.32% 29	21.05% 8	0.00% 0	2.63% 1	0.00% 0	38
The Environmental Health Officer was knowledgeable	68.42% 26	28.95% 11	2.63% 1	0.00% 0	0.00% 0	38
The Environmental Health Officer was professional	71.05% 27	26.32% 10	2.63% 1	0.00% 0	0.00% 0	38
You feel comfortable asking the Environmental Health Officer any questions about food safety and legislative requirements.	63.16% 24	34.21% 13	0.00% 0	2.63% 1	0.00% 0	38
The Environmental Health Officer clearly explained what is required to comply with the Food Act 2008 and Food Safety Standards	60.53% 23	36.84% 14	2.63% 1	0.00% 0	0.00% 0	38

The following comments were noted:

The City values your feedback. Do you have any other comments, concerns or suggestions that will help us to improve your experience with the City of Mandurah's Health Services?

- 1 *She is fabulous, tough enough to keep our chefs on their toes, respectfully.*
- 2 *Doing a great job, any queries I may have are answered immediately or followed up and answered.*
- 3 *I appreciate the information emails sent out by council have been able to create a Pest Control Plan and also found the last edition extremely helpful where to find information about allergens.*
- 4 *I find the department very easy to deal with and very professional.*
- 5 *Information circular informative and assisting to keep staff informed.*
- 6 *All of our safety assessments performed were very professional and to the point.*
- 7 *The Officer was excellent and very helpful in the process and very attentive at the work.*
- 8 *We're happy with service & the advice given.*
- 9 *The Officer was very helpful.*
- 10 *Very happy with every Officer that has visited.*

A similar survey is planned to be undertaken in 2020-21.

Statutory Environment

The *Food Act 2008* identifies local government entities as an enforcement agency that are responsible for the administration of the Act.

Section 8. Terms used

enforcement agency means —

- (a) the CEO; or
- (b) a local government

Section 118. Functions of enforcement agencies and delegation

(1) An enforcement agency has the functions in relation to the administration of this Act that are conferred or imposed on the agency by or under this Act or are delegated to the agency under this Act.

Policy Implications

Nil

Economic Implications

Nil

Risk Analysis

Food businesses proprietors are primarily responsible for ensuring the food they sell to the consumer is safe and suitable. The City has an important role in effectively regulating food businesses through ongoing monitoring, education and enforcement action.

The OAG states that weaknesses identified in the audit 'increase the risk that unsafe food practices are not rectified, and the public consumes hazardous food'.

The community would expect that the City has adequate resources and procedures in place to ensure an effective food safety regulation program is in place to reduce the risk of unsafe food being sold.

Strategic Implications

The following strategy from the City of Mandurah Strategic Community Plan 2020 – 2040 is relevant to this report:

Organisational Excellence:

- Ensure the City has the capacity and capability to deliver quality services and facilities through accountable and transparent business practices, governance, risk and financial management.

Conclusion

The City has reviewed the OAG's report on *Regulation of Consumer Food Safety by Local Government Entities*.

It is recommended that the Audit and Risk Committee note the City officers' comments outlined in the report.

NOTE:

Refer **Confidential Attachment 3.1** **OAG Food Safety Regulation Audit comparison with Local Government**

RECOMMENDATION

That the Audit and Risk Committee note the City responses in this report from the Office of the Auditor General's Report into Regulation of Consumer Food Safety by Local Government Entities as detailed in Confidential Attachment 3.1.

04	SUBJECT:	Office of the Auditor General: Working with Children Checks Managing Compliance
	DIRECTOR:	Director Strategy & Economic Development
	MEETING:	Audit & Risk Committee
	MEETING DATE:	8 September 2020

Summary

An audit conducted by the Office of Auditor General (OAG) recently made a number of recommendations that will impact on how the City of Mandurah will manage its requirements on Working with Children Checks. This audit assessed whether the WA health system, the Department of Justice and the Department of Education complied with their Working with Children Check obligations. The Auditor General's report can be viewed via the link <https://audit.wa.gov.au/reports-and-publications/reports/working-with-children-checks-compliance/>

Recommendations coming from the Audit require that all public sector entities who work with children, including those not sampled in this audit, should consider the findings in this report and implement the recommendations where appropriate, by 31 December 2020. The Office of Auditor General (OAG) have identified a number of recommendations.

The City of Mandurah have identified a number of areas that will require some modifications to our existing practices. These actions are identified in the body of the report. Council is requested to note the report and that a further report on progress will be provided to the Audit and Risk Committee in 2021.

Disclosure of Interest

N/A

Previous Relevant Documentation

N/A

Background

The OAG Audit on working with children has requested that all public sector entities who work with children should consider the findings of the OAG audit report and implement the recommendations made in the report.

The City of Mandurah has a number of work areas, roles or events where positions or employees will be covered by the Working with Children Card recommendations. There are current practices in place to manage the Working with Children requirements. The current practices have been reviewed against the recommendations and a number of changes will need to be made to be compliant with the recommendations by 31 December 2020.

Comment

The City has reviewed current Working with Children Card practices against the following recommendations made in the OAG report and those are detailed in Confidential Attachment 4.1.

OAG Recommendations

All public sector entities who work with children, including those not sampled in this audit, should consider the findings in this report and implement the recommendations where appropriate, by 31 December 2020. To ensure they manage their working with children obligations, all entities should:

1. Review their policies and procedures and communicate these to staff.
2. Ensure their Card records:
 - a) identifies all positions that require a Card and ensure that all individuals in those positions have a Card
 - b) capture sufficient information to track and monitor the Card status of all individuals, including Card number, surname, expiry date and where necessary, date of birth.
 - c) are complete and accurate
3. Ensure all Cards are valid by:
 - a) checking the Cards of all individuals against the Communities database, before they start working with children
 - b) registering new employees with Communities
 - c) re-checking all Cards, at least once per year
4. Monitor how they manage Card obligations through regular, detailed reporting on entity compliance to Executive.

The City of Mandurah has reviewed the recent OAG recommendations and has identified the current state of compliance and also actions required to meet compliance by December 31 2020 and the proposed actions are detailed in Confidential Attachment 4.1.

Policy Implications

In order to meet the requirements of the OAG recommendations the City will need to develop a CEO Policy and Procedure on Working with Children.

Strategic Implications

The following strategies from the *City of Mandurah Strategic Community Plan 2020 – 2040* are relevant to this report:

Social:

- Facilitate safe neighbourhoods and lifestyles by influencing the built form through urban design.
- Promote a positive identity and image of Mandurah and the contributions of its youth.

Conclusion

The City has reviewed the OAG's report on Working with Children Cards and reviewed compliance to its four recommendations. It has also proposed actions to comply with the recommendations by 31 December 2020. These proposed actions will be incorporated into the Office of the Auditor General – Improvements Tracking Report, which will be provided to the Audit and Risk Committee on a quarterly basis.

NOTE

- Refer ***Confidential Attachment 4.1*** ***Proposed Actions from the Recommendations from the WA Auditor General's Report – Working with Children Checks Managing Compliance***

RECOMMENDATION

That the Audit and Risk Committee note the City officer's responses and proposed actions to the Auditor General's report and Recommendations on Working with Children Cards as detailed in Confidential Attachment 4.1.

05	SUBJECT:	Occupational Safety and Health (OSH) 2019-2020 Annual Review
	DIRECTOR:	Director Strategy and Economic Development
	MEETING:	Audit and Risk Committee
	MEETING DATE:	8 September 2020

Summary

The City is now operating under our second 3-Year Strategic OSH Plan which was developed alongside the 2018 LGIS Worksafe Plan Audit outcomes and known legislative requirements. The 2019-2020 OSH performance is reflective of the considerable work completed in all business units within the City.

The Audit and Risk Committee and Council is requested to note the City's performance and progress being made in continuing the 3-Year Strategic OSH Plan and the initiatives being implemented to address the management of workplace injury.

Disclosure of Interest

N/A

Previous Relevant Documentation

- G.8/3/20 24 March 2020 Council noted the progress of the implementation of the 3-year Strategic OSH Plan and the City's current OSH performance for the YTD 2019/20 financial year.
- G.9/09/19 24 September 2019 Council noted the continuation of the 3-year Strategic OSH Plan 2019-2022 and the City's OSH performance for the 2018/19 financial year
- G.11/3/19 26 March 2019 Council endorsed the 3-year Strategic OSH Plan 2019-2022 and noted the OSH Key Performance Indicators
- G.30/3/16 22 March 2016 Council endorsed the City's 3-year OSH Plan

Background

Implementation of the Three-Year OSH Strategic Plan began in 2016. Since then, a range of actions have been planned and implemented to improve the City's OSH performance. The City is currently operating under the 2019-2021 OSH Strategic Plan.

Comment

The overview of the City's Occupational Safety and Health performance for 2019/20 is shown in confidential attachment 5.1.

Highlights of the 2019-2020 year include:

- In June 2020, Local Government Insurance Services (LGIS) were engaged to conduct an assessment into the City's Occupational Safety and Health (OSH) management systems. The assessment is scored against five elements and the final score received by the City was 82% which represents a LGIS Silver Diligence in Safety Award and is 10 points higher than the previous audit result conducted in 2018. A separate report on the audit is being considered at this Audit and Risk Committee meeting.

- Implementation of the OSH Contractor Management procedure which ensures both the City and contractors meet their respective OSH obligations. The procedure has started to rollout through the City and as at 31 July 2020 there has been over 200 contractors complete the online OSH induction.
- During COVID-19 shutdown the COVID-19 New Normal Back to Work Plan was created to assist the City to re-open safely. The plan was developed referencing Worksafe and WA Health Department requirements and was utilised by City employees to implement relevant actions to ensure compliance with legislation.
- Significant improvements have occurred in the City's OSH performance in 2019/20

Confidential attachment 5.1 details the City's OSH performance in more detail, however the highlights include:

- Lost time injuries have reduced from 14 in 2018-2019 to 8 in 2019-2020. The Councils benchmarked against reported 10 LTIs on average for the 2019-2020 financial year.
- The number of workers' compensation claims submitted have reduced from 45 in 2018-2019 to 27 in 2019-2020. The benchmarking Councils reported 35 claims for 2019-2020.
- The number of days lost have reduced from 1066 in 2018-2019 to 92 in 2019-2020. The benchmarking Councils reported 122 lost days on average for 2019-2020.

Statutory Environment

Nil

Policy Implications

Nil

Economic Implications

The City elected to pay a deposit rate insurance premium for the 2019/2020 financial year. The deposit premium rate is calculated at 2.2% of the estimated total salaries and wages (\$1,058,443) and provides the local government with the flexibility to not pay the maximum premium at the start of the financial year and effectively hold an estimated \$900K in the City's bank account rather than the insurers. If the workers compensation claims threshold for a financial year exceeds the amount that has been paid as a deposit premium, the insurer will call on the balance of the amount due, up to the maximum premium amount, which was \$1,924,442 (4% of total salaries) for the 2019/20 financial year. Where the workers compensation claims threshold for a financial year is below the amount that has been paid as a deposit premium, the insurer will pay the City the difference between the claims paid out (where the amount is over the minimum premium) or the minimum premium (where the claims amount is under the minimum premium, \$890,054 – 1.85%) and the deposit premium amount of \$1,058,443.

Once the 2019/2020 workers compensation claims are finalised, the City is expecting it will receive a refund for the 2019/2020 fund year as the deposit rate insurance premium is below the claims amount that is estimated to be paid out. Any refunds received by the City will be transferred to the Workers Compensation Reserve that was created in the 2019/2020 for the purpose of funding previous years workers compensation claim that are open and still have costs required to be paid by the City of Mandurah (these are not included in the current budget that is approved by Council).

The benefits for having proficient OHS systems in place include employees feeling safe carrying out their work; the organisation demonstrating and committing to a safe work culture; and reduced maximum insurance premium percentages (resulting in the maximum amount paid in one year regardless of the dollar value of claims).

Risk Analysis

N/A

Strategic Implications

The following strategies from the *City of Mandurah Strategic Community Plan 2020 – 2040* are relevant to this report:

Health:

- Provide quality health and wellbeing programmes and services that target whole of life health from infants to seniors.
- Promote the importance of a healthy, active lifestyle and the role the natural environment plays in preventative health, within our community.

Organisational Excellence:

- Build and retain a skilled, agile, motivated and healthy workforce.
- Ensure the City has the capacity and capability to deliver quality services and facilities through accountable and transparent business practices, governance, risk and financial management.
- Ensure that our actions maintain a sustainable balance between economic growth, the environment and social values.

Conclusion

The City has progressively been implementing the actions of the 3-Year OSH Plan and the Audit and Risk Committee and Council is requested to note the progress of the implementation of the plan and also note the OSH performance for the 2019/20 year.

NOTE:

- Refer ***Confidential Attachment 5.1*** ***City of Mandurah OSH Performance Overview for the 2019 – 2020 financial year***

RECOMMENDATION

That the Audit and Risk Committee

1. Notes the City's OSH performance for the 2019/20 financial year as detailed in Confidential Attachment 5.1.
2. Notes the progress of implementation of the 3-Year Strategic OSH Plan.

06	SUBJECT:	2020 Local Government Insurance Services 3 Steps to Safety Program
	DIRECTOR:	Director Strategy and Economic Development
	MEETING:	Audit and Risk Committee
	MEETING DATE:	8 September 2020

Summary

In June 2020, Local Government Insurance Services (LGIS) were engaged to conduct an assessment into the City's Occupational Safety and Health (OSH) management systems.

This report provides a summary of the assessment outcomes and the Audit and Risk Committee and Council are requested to acknowledge the audit result and the proposed actions as a result of the audit findings.

Disclosure of Interest

N/A

Previous Relevant Documentation

- G.30/3/16 22 March 2016 Council endorsed the City's 3-year OSH Plan

Background

LGIS have been engaged by the City for several years to aid the development and improvement of the City's OSH performance and management systems. As part of the assistance provided, LGIS have been regularly engaged to provide reviews and audits of the OSH management system.

Two recent OSH system reviews have included a full 3 Step to Safety Program assessment which was completed in August 2018. The City achieved 72% which provided a good benchmark and assisted with the development of the 2019-2021 3 Year Strategic OSH Plan. In February 2020, LGIS conducted a desktop assessment prior to the most recent audit, which showed the City was on track to improve on the August 2018 assessment results.

Comment

The LGIS 3 Step to Safety Program which was utilised for the June 2020 assessment comprises of 5 elements each of the elements have a number of indicators that are used to measure achievements. The assessment involved visiting the Administration Centre, MARC, Operations Centre, Southern Depot, Dog Pound, Roads Construction site, Seniors and Community Centre, Rangers, Billy Dower Youth Centre and CASM and involved interviews and observations with a broad cross section of the organisation. The assessment was also peer reviewed by another member of the LGIS OSH team. The table below includes each of the elements, performance expected, the City's assessment results and a summary of key proposed actions.

Element	Performance expected	Score	Summary of proposed actions
Management Commitment	There is commitment to achieving high standards of safety and health performance through effective safety management.	95%	<ul style="list-style-type: none">Develop relevant training packages with the focus on refresher training.Ensure CEO OSH&W Policy is reviewed every year.Develop processes to communicate OSH&W policy to contractors.

			<ul style="list-style-type: none"> • Display OSH Policy in key customer interfaces.
Planning	Planning is used to establish and maintain an integrated safety and health management system that is set up to continuously improve safety and health performance across all operational activities.	81%	<ul style="list-style-type: none"> • Develop OSH objectives. • Identify the requirement for additional OSH procedures. • Develop & implement procedures for people with special needs. • Train people who are responsible for contractors and review staff understanding regularly. • Ensure all emergency evacuation drills are documented. • OSH Contractor Management procedure is embedded into the City's onboarding processes and management of contractors. • Develop OSH work instructions for all work activities and managers to ensure staff are aware to follow these.
Consultation and Reporting	Mechanisms are in place for consultation and reporting on safety and health matters and are working effectively.	89%	<ul style="list-style-type: none"> • Implement the One Council hazard reporting system. • Review consultative mechanisms.
Hazard Management	An effective system is in place to identify hazards, assess and control risks associated with the organisation's activities, processes, products or services.	68%	<ul style="list-style-type: none"> • Complete risk registers for all departments. • Review corporate induction presentation to include detail on hazard reporting process. • Develop priorities for identified controls. • Staff to be fully trained on hazard identification and how to undertake risk assessments. • Undertake periodic reviews of the effectiveness of hazard identification, risk assessment and risk control processes. • Develop and implement a process to ensure that risk assessments are completed on identified hazards.
Training and Supervision	Training and supervision is organised to reduce the risk of work-related injury and disease and is evaluated to ensure its effectiveness.	79%	<ul style="list-style-type: none"> • Complete review of the OSH training procedure to include competency-based assessments. • Promote the OSH training plan. • Training needs analysis document to be included into OneCouncil which will assist the identification of training required and completed.
Overall score		82%	

Statutory Environment

Although an external audit is not included as a specific requirement under the Western Australian Occupational Safety and Health Act 1984 and Occupational Safety and Health Regulations 1996 there is an expectation that all elements of an occupational safety and health management system are reviewed.

Policy Implications

N/A

Economic Implications

N/A

Risk Analysis

Actions arising from the LGIS 3 Step to Safety Program assessment will be included in the 2019-2021 3-Year Strategic OSH Plan and also the 2022-2024 3-Year Strategic OSH Plan as it is developed over the next 12 months. The expectation is that each of the identified actions will have a positive impact on the 2022 LGIS 3 Step to Safety Program assessment, the City's workers' compensation claims costs and the OSH Management system.

Strategic Implications

The following strategies from the *City of Mandurah Strategic Community Plan 2020 – 2040* are relevant to this report:

Organisational Excellence:

- Build and retain a skilled, agile, motivated and healthy workforce.
- Ensure the City has the capacity and capability to deliver quality services and facilities through accountable and transparent business practices, governance, risk and financial management.
- Ensure that our actions maintain a sustainable balance between economic growth, the environment and social values.

Conclusion

The City has placed considerable finance, time and development into the existing OSH management system. The LGIS 3 Step to Safety Program June 2020 assessment result is testament to the City's commitment to consistently review and improve our OSH management systems.

NOTE:

- Refer ***Confidential Attachment 6.1 LGIS 3 Steps to Safety Program Assessment June 2020***

RECOMMENDATION

That the Audit and Risk Committee

- 1. Acknowledges the success of the City's OSH LGIS 3 Steps to Safety Program assessment report score of 82%**
- 2. Notes the proposed actions as a result of the assessment**
- 3. Notes the current 3-year OSH plan will be updated based on the identified actions from the assessment.**