Audit and Risk Committee Meeting

4 October 2021

Agenda

Notice is hereby given of the Audit and Risk Committee Meeting to be held in the Council Chambers, City of Kwinana Administration Centre commencing at 5:30pm.

Wayne Jack
Chief Executive Officer

Members of the public who attend Council meetings should not act immediately on anything they hear at the meetings, without first seeking clarification of Council's position. Persons are advised to wait for written advice from the Council prior to taking action on any matter that they may have before Council.

Agendas and Minutes are available on the City's website www.kwinana.wa.gov.au

TABLE OF CONTENTS

1 Opening and announcement of visitors

Presiding Member to declare the meeting open and welcome all in attendance.

2 Acknowledgement of country

Presiding Member to read the Acknowledgement of county

"It gives me great pleasure to welcome you all here and before commencing the proceedings, I would like to acknowledge that we come together tonight on the traditional land of the Noongar people and we pay our respects to their Elders past and present."

3 Attendance, apologies, Leave(s) of absence (previously approved)

Apologies

Leave(s) of Absence (previously approved):

4 Declarations of Interest (financial, proximity, impartiality – both real and perceived) by Members and City Officers

Section 5.65(1) of the *Local Government Act 1995* states:

A member who has an interest in any matter to be discussed at a council or committee meeting that will be attended by the member must disclose the nature of the interest —

(a) in a written notice given to the CEO before the meeting; or
(b) at the meeting immediately before the matter is discussed.

Section 5.66 of the *Local Government Act 1995* states:

If a member has disclosed an interest in a written notice given to the CEO before a meeting then —

(a) before the meeting the CEO is to cause the notice to be given to the person who is to preside at the meeting; and
(b) at the meeting the person presiding is to bring the notice and its contents to the attention of the persons present immediately before the matters to which the disclosure relates are discussed.

5 Confirmation of minutes

5.1 Audit Committee Meeting held on 14 June 2021:

COMMITTEE DECISION

###

MOVED CR **SECONDED CR**

That the Minutes of the Audit Committee Meeting held on 14 June 2021 be confirmed as a true and correct record of the meeting.

6 Reports

6.1 Occupational Safety and Health (OSH) Statistical Data Report and the Gap Analysis Desktop Audit to ISO 45001:2018 (Health and Safety Management Systems) Report

SUMMARY:

This statistical data is provided to the Audit and Risk Committee for noting.

Council has endorsed a Health and Safety Policy to meet its moral and legal obligation to provide a safe and healthy work environment for all employees, contractors, customers and visitors. This commitment extends to ensuring the City's operations do not place the community at risk of injury, illness or property damage. At every Audit and Risk Committee Meeting the Committee receives a report detailing statistical data. This report entitled the City of Kwinana OSH Statistical Data Report is enclosed as Attachment A.

Over the past twelve months, the City has progressed the Safety and Health Management System framework. This includes the Tier Documentation and the OSH Management Plan. With the recent introduction of the Work Health and Safety legislation, the City engaged an external consultant to undertake a desktop audit of the City's Safety framework. A gap analysis of the framework was performed in June 2021 with the objective of the gap analysis to determine the City's adherence of the documentation to ISO 45001:2018 Occupational Health and Safety Management Systems (45001).

The audit confirmed that the City's OHSMS provides a high level of compliance. There were some areas of improvement identified with primary recommendations to conduct an annual risk assessment workshop and an annual management review forum.

The report entitled OHSMS Gap Analysis ISO 45001:2018 Health and Safety Management Systems for City of Kwinana is enclosed as Attachment B.

OFFICER RECOMMENDATION:

That the Audit and Risk Committee note:

1. **City of Kwinana OSH Statistical Data Report detailed in Attachment A.**
2. **OHSMS Gap Analysis ISO 45001:2018 Health and Safety and Health Management Systems for the City of Kwinana Report detailed in Attachment B.**

6.1 OCCUPATIONAL SAFETY AND HEALTH (OSH) STATISTICAL DATA REPORT AND THE GAP ANALYSIS DESKTOP AUDIT TO ISO 45001:2018 (HEALTH AND SAFETY MANAGEMENT SYSTEMS) REPORT

DISCUSSION:

The OSH Statistical Data Report is provided to the Audit and Risk Committee at each Audit and Risk Committee Meeting. The City assesses the incident reporting data to provide information on the nature and extent of injury and/or disease, including a comprehensive set of data for the workplace, to assist in the efficient allocation of resources, to identify appropriate preventative strategies and monitor the effectiveness of these strategies and to provide a set of data for benchmarking against other Local Governments. As a result, the City can adequately identify, evaluate and manage the safety and health aspects of its workforce operations.

Summary of Statistical Data:

The statistical data report details information over a three-month period, 1 June 2021 to 31 August 2021. From the represented data, it is noted an increase in incident frequency trend with three incidents reported in June, five incidents in July and six incidents in August with the total for the period at fourteen.

Five from the City Life directorate, four from the City Development and Sustainability directorate, four from the City Infrastructure directorate and one from the Office of the CEO. The departments that are domiciled to each directorate includes teams that are considered “high risk” teams due to their operational nature. The incidents reported over the three-month reporting period have occurred in these “high risk” teams. Three of the incidents were listed as Injury – no lost time, three medical treatments, two first aid, two near misses, and four reports only. (Noting, the statistical representation of the incident data has been amended to reflect the City’s recently updated organisational structure.)

OHSMS Gap Analysis ISO 45001:2018 Health and Safety Systems Report:

Further to the introduction of the new Health and Safety legislation and the development of the City’s Safety and Health Management System framework ,the City engaged an external consultant to undertake a desktop audit of the City’s documentation to determine whether the framework will provide a structured approach to the City’s safety and health activity, meet legislative requirements for safety and health, minimise overall risk from the City’s perspective and promote continuous improvement in safety and health performance. A gap analysis was performed with the objective being to determine adherence of the City’s documentation to ISO 45001:2018 Occupational Health and Safety Management Systems (45001).

Overall, the audit confirmed that the City’s Safety and Health Management System framework provided a high level of compliance to the majority of the clauses contained in ISO 45001:2018. However, there were two areas assessed that would not comply with the standard and both of the areas have been rated as a high priority. This first area for improvement recommended that an annual risk assessment workshop is undertaken to ensure that all the City’s OSH risks are identified and appropriately controlled. This process to be included in the City’s Safety and Health Management System framework.

6.1 OCCUPATIONAL SAFETY AND HEALTH (OSH) STATISTICAL DATA REPORT AND THE GAP ANALYSIS DESKTOP AUDIT TO ISO 45001:2018 (HEALTH AND SAFETY MANAGEMENT SYSTEMS) REPORT

The second opportunity for improvement was the inclusion of an annual management review forum to ensure that the City's Safety and Health Management System framework is reviewed and continually improved upon. This process should also be included in the framework. In addition, contained within the report are further opportunities for improvements, noting that the City's Safety and Health Management System framework does essentially meet the requirements of the standard.

In order to address the first clause, whereby the framework does not satisfy the requirements, the City has scheduled a workshop for 23 September 2021, facilitated by the author of the desktop audit report. (Noting, there will be several workshops to ensure that the all areas of the organisation are providing input to identifying risks and hazards and that these are appropriately controlled.) The workshops will have representation from Executive, Senior Management, Supervisors, Safety Representatives and Officer level with the initial workshop attendees from the identified "high risk" teams.

At the workshops, it is also intended to establish a process (as per the requirements of ISO 45001:2018) for the formal management review of the safety framework which will address the identified second opportunity for improvement. The outcomes from the workshops will be reported to the Audit and Risk Committee.

<u>OSH System Assessment:</u>

Since July 2020, the City has been actively reviewing and implementing the Safety and Health Management framework across the organisation. As part of the development of the framework, there has been a requirement to continually assess and advance processes, improve on the information obtained and collate data that provides meaningful evaluation thereby assisting in the appropriate management of hazards and risks at the City. Whilst there has been substantial progression, this has been achieved, reported and monitored through various manual and often laborious recording systems. It is now an appropriate time for the City to investigate an electronic system that will assist with efficiencies, streamlining the current processes and providing the opportunities for further enhancements to the City's framework and performance.

The City has commenced research into an appropriate electronic system having viewed a couple of potential products. Until the scheduled hazard and risk workshops are undertaken and outcomes determined, the exact requirements for an electronic system can not be finalised. It is envisaged that workshops will provide the information pertaining to the functionality, suitability and alignment of an electronic system to the City's current framework and future needs. (Noting, that it is for this reason that further information and trending of data, including the incident frequency rates, have not been included in the statistical data contained within Attachment A. The intention is this will be included as part of an electronic system).

As part of the research and review into an appropriate electronic system, there will be need to be consideration to funding the implementation of a new system, noting that the City's current Occupational Health and Safety budget has not factored any expenditure in this area. If the City progresses with the new system, there will be a requirement to identify potential funding sources.

6.1 OCCUPATIONAL SAFETY AND HEALTH (OSH) STATISTICAL DATA REPORT AND THE GAP ANALYSIS DESKTOP AUDIT TO ISO 45001:2018 (HEALTH AND SAFETY MANAGEMENT SYSTEMS) REPORT

Further Developments relating to Safety and Health at the City:

The City is currently exploring the opportunity to participate in an integrated program or shared services with other Local Government that participate in the "Gap Group of Councils".
The focus of the sharing of services is within the Safety and Health area and it is envisaged that LGIS (Local Government Insurance Services) will facilitate the program.

LEGAL/POLICY IMPLICATIONS:

Regulation 17 of the Local Government (Audit) Regulations 1996 provides:

17. CEO to review certain systems and procedures

(1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to —
(a) risk management; and
(b) internal control; and
(c) legislative compliance.
(2) The review may relate to any or all of the matters referred to in subregulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.
(3) The CEO is to report to the audit committee the results of that review.

FINANCIAL/BUDGET IMPLICATIONS:

The financial implications as a result of this report include the purchase/implementation of an electronic safety system.

ASSET MANAGEMENT IMPLICATIONS:

There are no asset management implications as a result of this report.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no environmental implications as a result of this report.

There are no implications on any determinants of health as a result of this report.

6.1 OCCUPATIONAL SAFETY AND HEALTH (OSH) STATISTICAL DATA REPORT AND THE GAP ANALYSIS DESKTOP AUDIT TO ISO 45001:2018 (HEALTH AND SAFETY MANAGEMENT SYSTEMS) REPORT

STRATEGIC/SOCIAL IMPLICATIONS:

This proposal will support the achievement of the following outcome and objective detailed in the Corporate Business Plan.

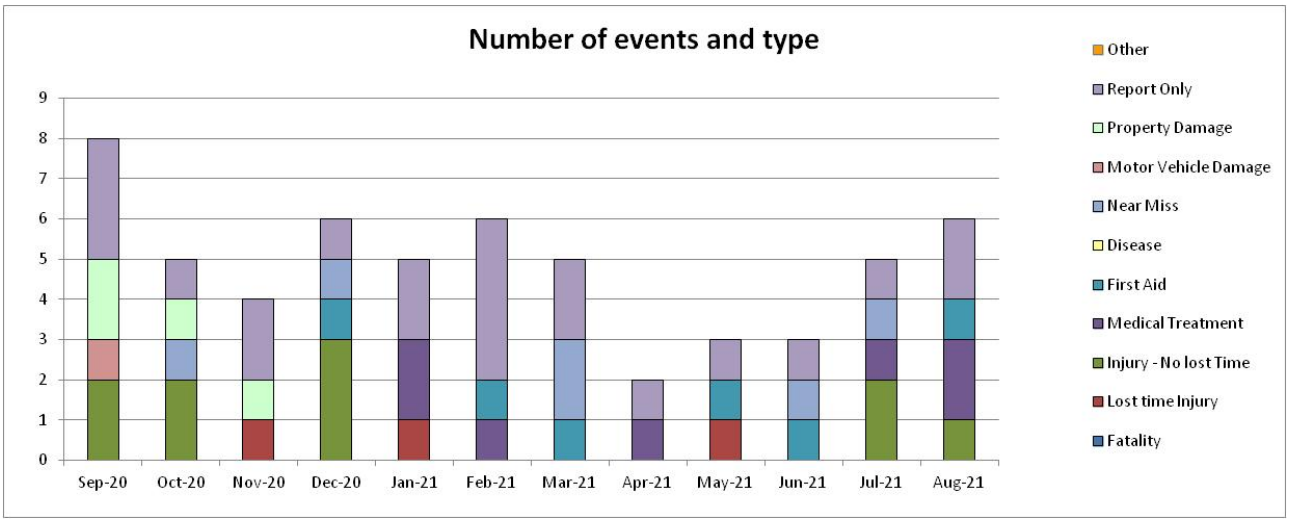
Plan	Outcome	Objective
Corporate Business Plan	Business Performance	7.1 Attract and retain a high quality, motivated and empowered workforce so as to position the organisation as an "Employer of Choice"

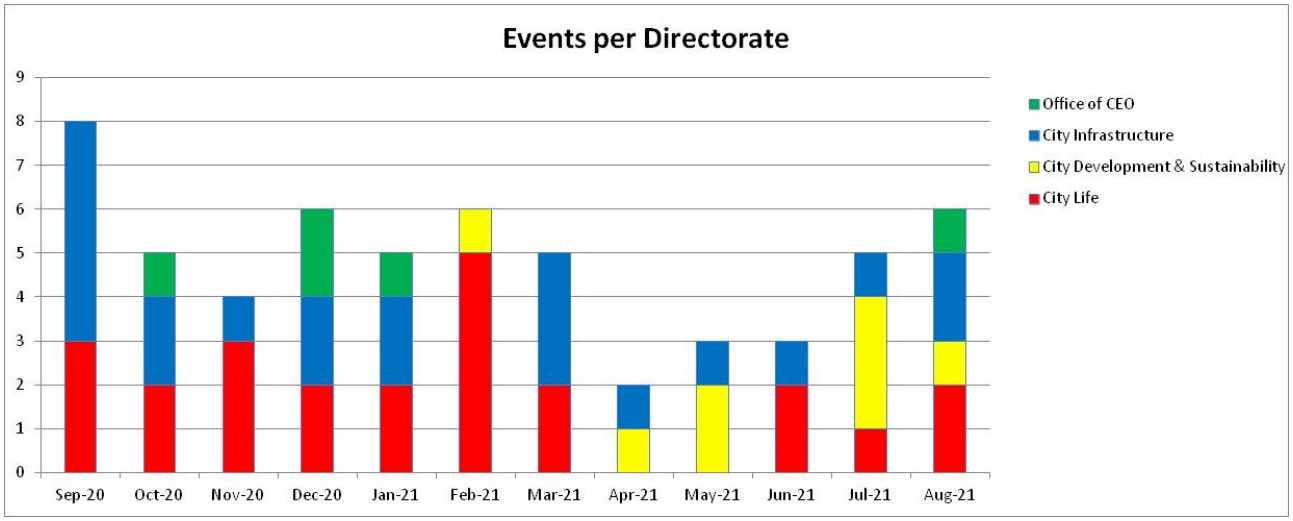
COMMUNITY ENGAGEMENT:

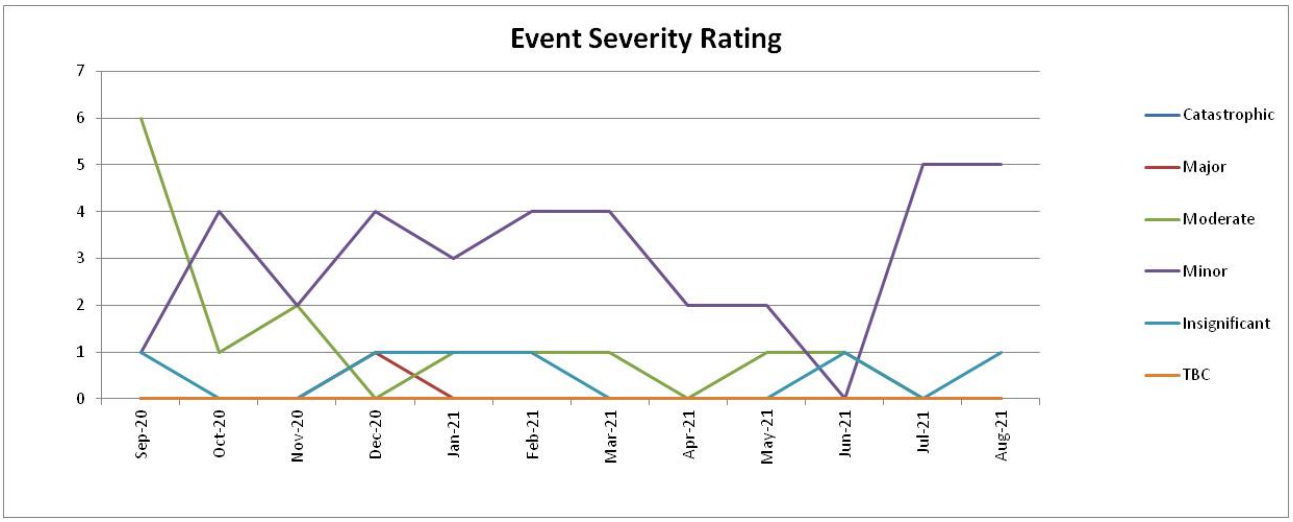
There are no community engagement implications as a result of this report.

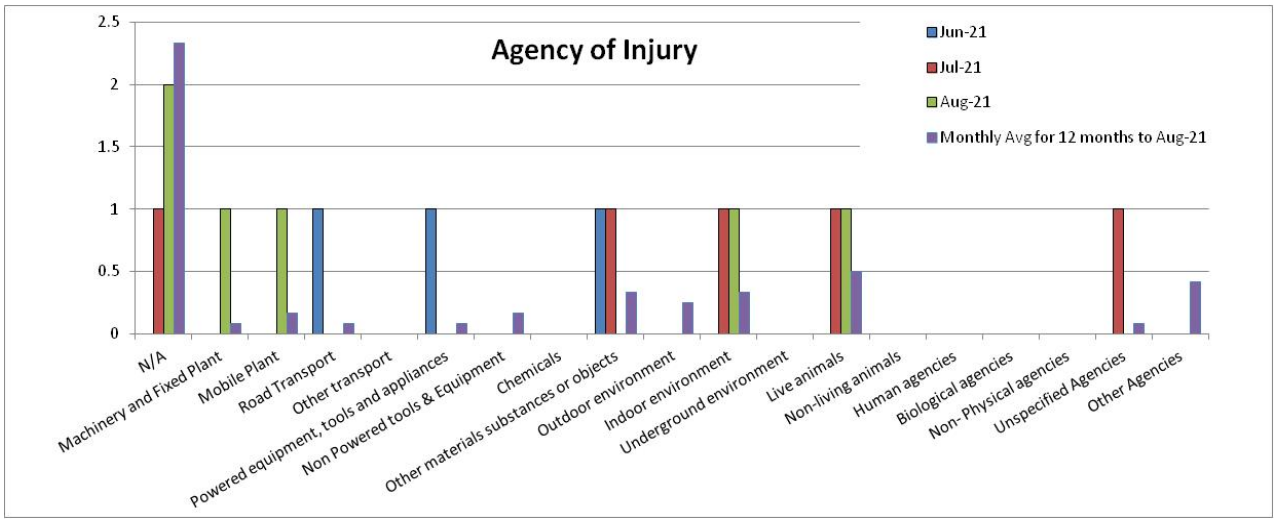
ATTACHMENT A

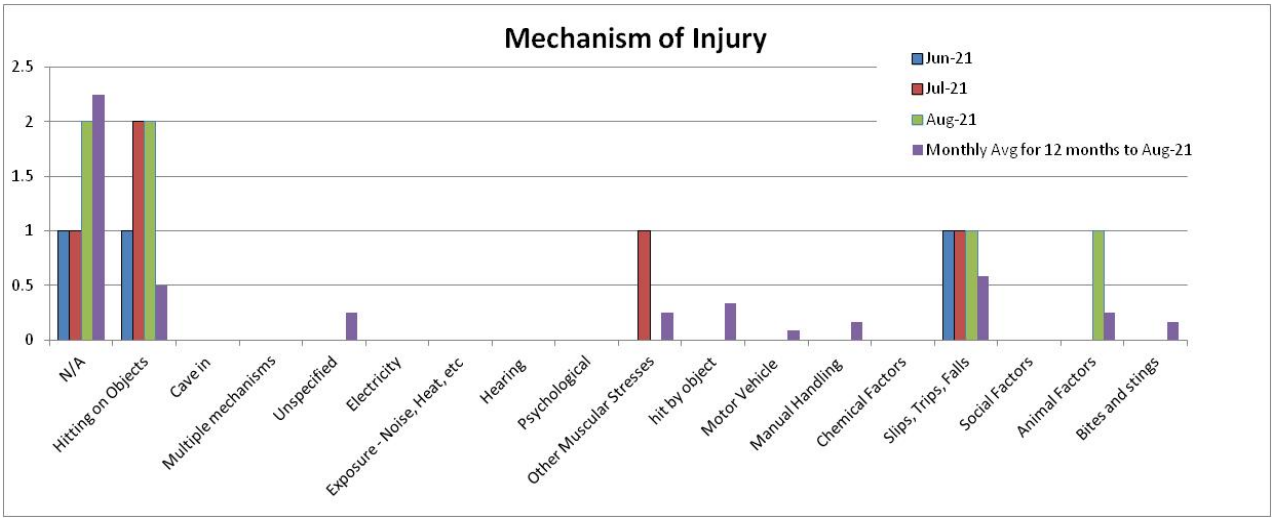
City of Kwinana - OSH Statistical Data Report - 31 August 2021

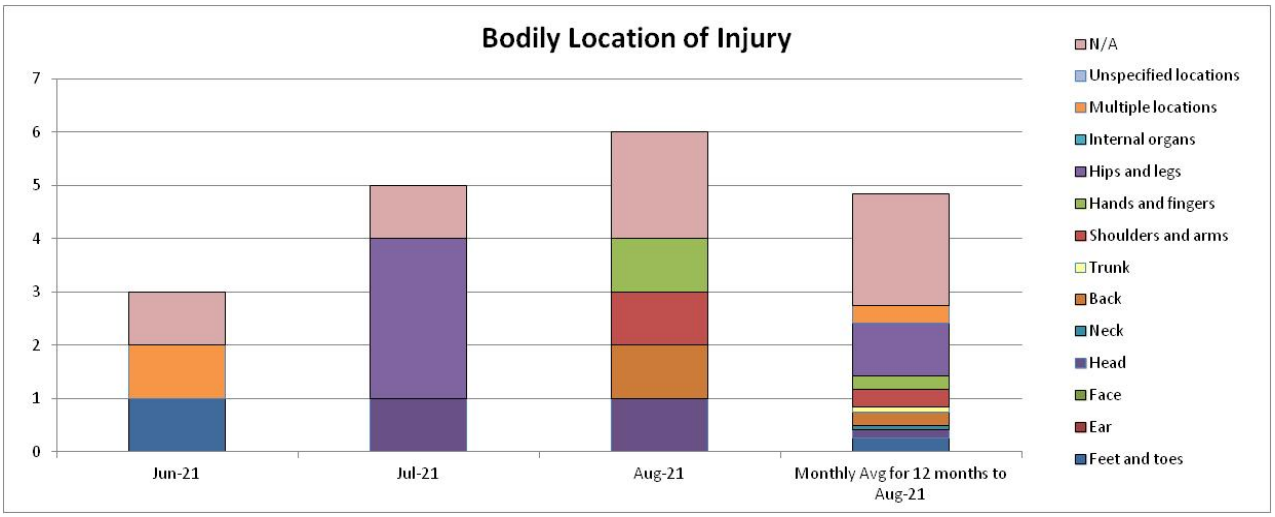


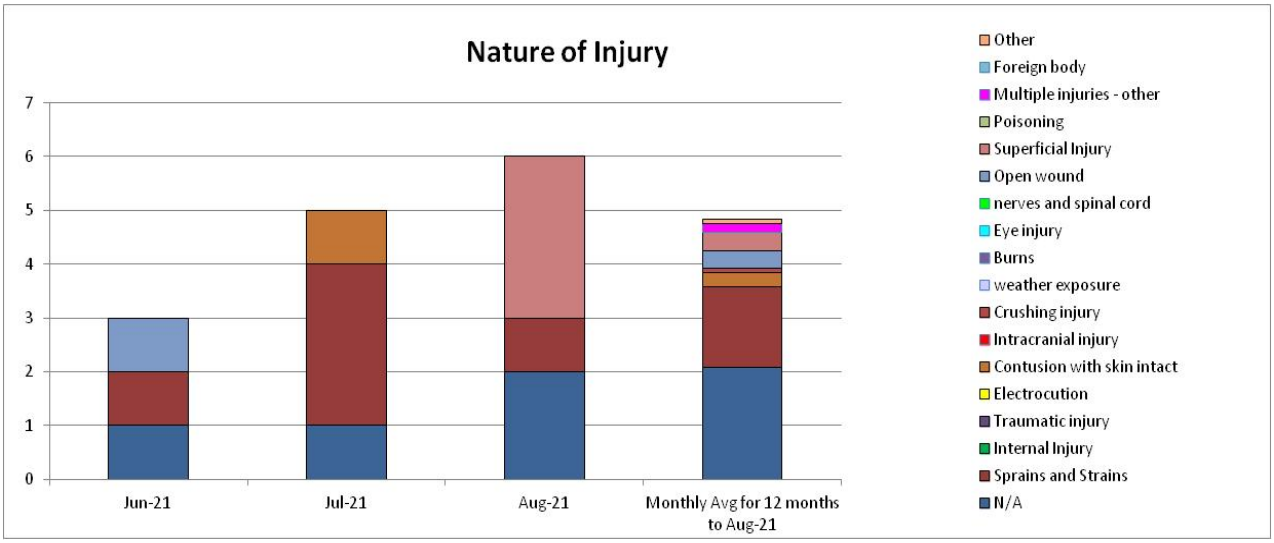


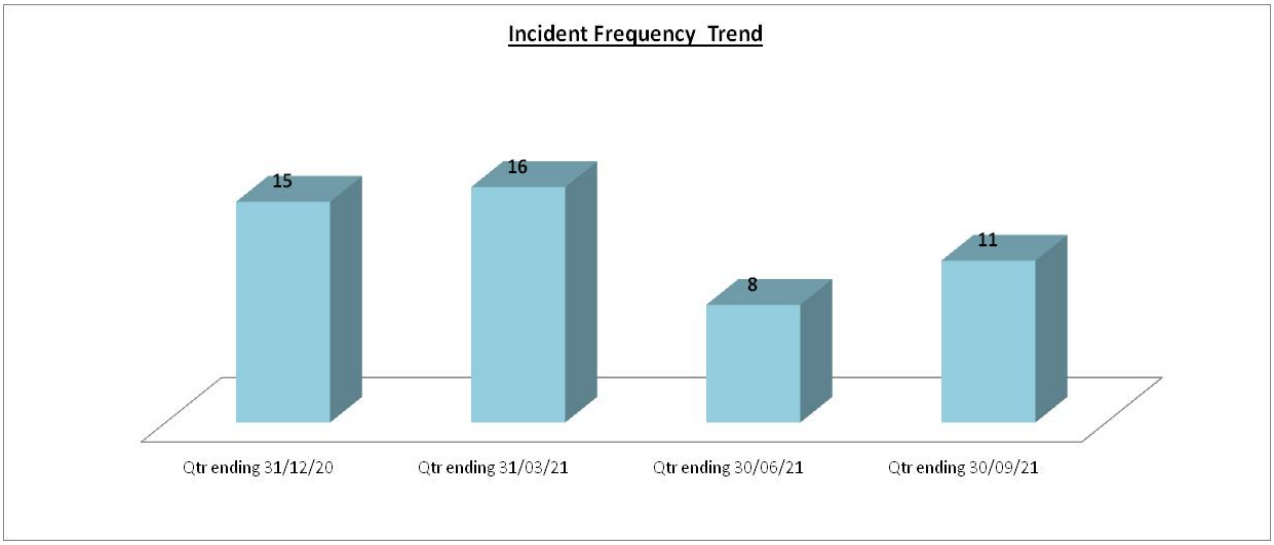


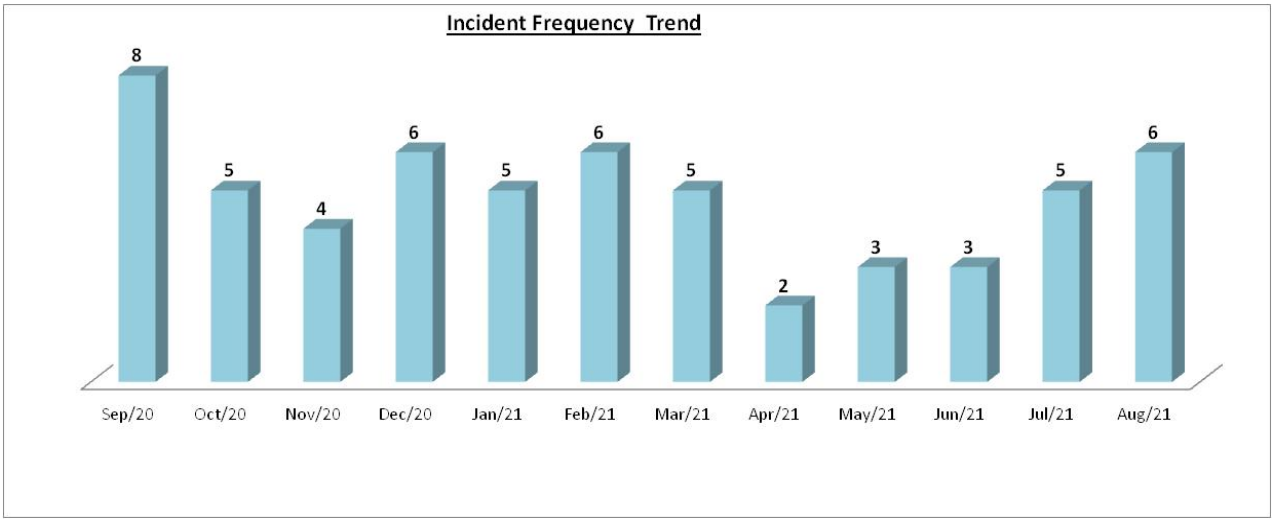

Agency of Injury
Jun-21
Jul-21
Aug-21
Monthly Avg for 12 months to Aug-21
2.5
2
1.5
1
0.5
0
N/A
Machinery and Fixed Plant
Mobile Plant
Road Transport
Other transport
Powered equipment, tools and appliances
Non Powered tools & Equipment
Chemicals
Other materials substances or objects
Outdoor environment
Indoor environment
Underground environment
Live animals
Non-living animals
Human agencies
Biological agencies
Non- Physical agencies
Unspecified Agencies
Other Agencies


Mechanism of Injury
Jun-21
Jul-21
Aug-21
Monthly Avg for 12 months to Aug-21
2.5
2
1.5
1
0.5
0
N/A
Hitting on Objects
Cave in
Multiple mechanisms
Unspecified
Electricity
Exposure - Noise, Heat, etc
Hearing
Psychological
Other Muscular Stresses
hit by object
Motor Vehicle
Manual Handling
Chemical Factors
Slips, Trips, Falls
Social Factors
Animal Factors
Bites and stings


Bodily Location of Injury
7
6
5
4
3
2
1
0
Jun-21
Jul-21
Aug-21
Monthly Avg for 12 months to Aug-21
N/A
Unspecified locations
Multiple locations
Internal organs
Hips and legs
Hands and fingers
Shoulders and arms
Trunk
Back
Neck
Head
Face
Ear
Feet and toes


Nature of Injury
7
6
5
4
3
2
1
0
Jun-21
Jul-21
Aug-21
Monthly Avg for 12 months to Aug-21
Other
Foreign body
Multiple injuries - other
Poisoning
Superficial Injury
Open wound
nerves and spinal cord
Eye injury
Burns
weather exposure
Crushing injury
Intracranial injury
Contusion with skin intact
Electrocution
Traumatic injury
Internal Injury
Sprains and Strains
N/A


Incident Frequency Trend
15
16
8
11
Qtr ending 31/12/20
Qtr ending 31/03/21
Qtr ending 30/06/21
Qtr ending 30/09/21


Incident Frequency Trend
8
5
4
6
5
6
5
2
3
3
5
6
Sep/20
Oct/20
Nov/20
Dec/20
Jan/21
Feb/21
Mar/21
Apr/21
May/21
Jun/21
Jul/21
Aug/21

GFG CONSULTING
ABN 94 156 452 050

OHSMS Gap Analysis
ISO 45001:2018 Health and Safety Management Systems

FOR

CITY OF KWINANA

DATE: 27th July 2021

REFERENCE: Q14062021-001

DOCUMENT CONTROL RECORD

Prepared By:	Hennah Brnjak
Position:	OHS Consultant
Signed:	
Date:	27/07/2021

Approved By:	Paul Owen
Position:	**Business Operations Manager**
Signed:	
Date:	27/07/2021

REVISION STATUS

Revision No.	Description of Revision	Date	Approved
V1	Draft to issue to client	14/07/2021	
V2	Amendments to client queries	27/07/2021	

Recipients are responsible for eliminating all superseded documents in their possession.

DISCLAIMER

This document is published in accordance with and subject to an agreement between Glen Flood Group Pty Ltd (trading as GFG Consulting) and the City of Kwinana. It is confined to the issues that have been raised by the Client in the Client's engagement of GFG Consulting and is prepared using the standard of skill and due care ordinarily exercised by management and business consultants in preparing such documents.

Any person or organisation that relies on or uses the document for reasons or purposes other than those agreed by GFG Consulting and the Client without first obtaining the prior written approval of GFG Consulting, does so entirely at their own risk. To the extent permitted by law, GFG Consulting excludes any liability, including any liability for negligence, for any loss, including indirect or consequential damages arising from or in relation to any reliance on this document for any purpose other than that agreed with the Client.

ACKNOWLEDGEMENT

GFG Consulting would like to thank Sue Wiltshire for the opportunity to assist with the auditing of the City of Kwinana Occupational Health and Safety Management System.

Contents

1. Preliminary Audit Overview and Examiner's Statement

A gap analysis was performed on City of Kwinana's (CoK) Occupational Health and Safety Management System (OHSMS) in June 2021. The objective of the gap analysis is to determine adherence of the CoK OHSMS documentation to ISO 45001:2018 Occupational health and safety management systems (45001).

Overall, the audit confirmed that the City's OHSMS provides a high level of compliance to the majority of the 45001 clauses. However, some areas for improvement were identified. It is recommended that an annual risk assessment workshop is undertaken to ensure that all the City's OHS risks are identified and appropriately controlled. The process for this workshop should be documented within the OHSMS. Additionally, an annual management review forum would be beneficial to ensure that the OHSMS is reviewed and continually improved upon. This process should also be documented within the OHSMS. There are also further opportunities for improvement which are noted within the report.

In addition to the recommendations to meet specific clauses of 45001, the OHSMS could be improved by ensuring that each document within the system provides information on the parent-child relationship. For example, a risk assessment procedure would make reference to both the risk management policy (parent) and safe work method statement (child). This ensures that personnel within each business unit understand their responsibilities with regards to implementation of the OHSMS.

A table which provides an overview of all recommendations can be found in section 4.0.

2. Scope

This gap analysis reviews the City's OHSMS for compliance to all clauses of 45001. This is a desktop audit only and does not assess compliance to the OHSMS.

The following documentation was reviewed:

- Safety and Health Management Framework - Tier 1
- Safety and Health Management Framework - Tier 2
- Attachment B - Safety and Health Management Framework Tier 3 - Final - 12 May 2021
- OSH Management Action Plan - 2021 – 2023
- Risk register (City Operations)
- Index of Essential Services/Rangers documentation
- Recquatic Document Approval Process (spreadsheet)
- Volunteers Documentation
- OSH Contractor documentation

3. ISO 45001 – Gap Analysis

3.1. Determining the scope of the OH&S management system (4.3 - ISO 45001:2018)

3.1.1. Document Review Analysis

The Safety and Health Policy as well as relevant sections of the Tier Documentation (Tier 1 & 2 - Section 1 to 1.3, Tier 3 - Page 3-6) clearly identifies its responsibility for the safety and health of 'all persons employed or engaged by the City' and its commitment to achieving zero harm within the City's working environment.

The policy states its responsibilities under the WA Occupational Safety and Health Act (1984) and associated legislations.

The safety control pillars provide a good summary of the scope of the OHSMS and how risks within the City are identified and controlled by implementing risk analysis procedures in a consultative manner.

3.1.2. ISO 45001:2018 Compliance Assessment

Yes. The City's OHSMS meets the requirements of 45001.

3.1.3. Recommendations

None. As this references the broad scope of the OHSMS, there are no recommendations for this clause. Recommendations will be provided throughout this document, below.

3.2. OH&S Policy (5.2 - ISO 45001:2018)

3.2.1. Document Review Analysis

The Safety and Health Policy is current and included within all Tiers of the system. As mentioned above, the City's policy clearly defines its obligation under relevant Acts and regulations.
The Policy clearly commits to consultation with management and workers through engagement in several ways including the City's OSH Committee and safety and health representatives.

The CoK's OHS policy is detailed and includes its commitment to meet its duties of providing a safe and healthy work environment for all its stakeholders.

The policy details the City's commitment to legal requirements by identifying and reducing associated risks, internal and external consultation as well as internal review to continually improve upon the OHSMS.

3.2.2. ISO 45001:2018 Compliance Assessment

Yes. The City's OHSMS meets the requirements of 45001.

3.2.3. Recommendations

None.

3.3. Organisational Roles, Responsibilities and Authorities (5.3 - ISO 45001:2018)

3.3.1. Document Review Analysis

The responsibilities and authorities within the OHSMS are clearly defined within the Tier 1 Document in section 2.2 Leadership and accountability.

Responsibility of each position within CoK's organisational structure with regards to all key aspects of OHS – risk management, incident & accident as well as emergency management are well defined in all three Tier Documents.

The emergency procedure defines external stakeholders of the City's organisational responsibilities by referencing the roles of external stakeholders as state agencies and local authorities in Tier 1 Documentation (1.3 Definitions).

3.3.2. ISO 45001:2018 Compliance Assessment

Yes. The City's OHSMS meets the requirements of 45001.

3.3.3. Recommendations

The City's OHSMS defines overarching responsibilities for health and safety, however it does not include details of exactly how incidents, hazards, audit findings etc. are reported and to who they are reported. For example, how does the organisation ensure that information from the various safety feedback pathways (i.e. near misses, incidents, minutes of safety toolbox talks etc.) are tracked, reviewed, and fed back down to other business units? The addition of some flow charts/procedures which define the processes for unwanted event reporting and investigation and corrective actions would be helpful.

Additionally, defining which positions will be classed as 'Officers' under the new WHS legislation could be discussed at the annual management review forum (i.e. CEO, Directors & Senior Managers? This will depend on how the roles influence the organisation, i.e. what type of decisions the role can make & how much authority they have in terms of deciding where resources/finances are allocated).

3.4. Hazard identification (6.1.2 - ISO 45001:2018)

3.4.1. Document Review Analysis

The City's OHSMS includes processes to identify hazards. Tier 1, Section 3.1 Hazard and Risk Management Identifies the overall process for risk assessment and reporting. Key Performance Requirements are included and the document states that all hazards and risks are to be systematically identified.

Tier 2 (section 1.2) introduces the City's risk matrix and references the City's risk management policy D15/57852. Section 3.1 Hazard and Risk Management provides comprehensive details on risk and hazard identification and control measures. The way in which the process is verified to ensure corrective actions are identified and closed out is also described.

Tier 3 document (City Risk Assessment Process, page 11) identifies the way in which control measures are assessed and implemented as well as how opportunities for improvement are identified (Section 3.4 Change Management Standard of Tier 2 Document).

Tier 1 references the City's legal commitment and responsibilities with regards to general statutory obligations, OHS Policy (Section 1); plant, and equipment as well as contractor management responsibilities (Section 3.2 Safely Controlling Operations).

3.4.2. ISO 45001:2018 Compliance Assessment

Yes. A good framework for hazard identification, control and review are provided. There is a clear framework for how to address identified risks within the organisation. The manner in which legal requirements are met is also described (Tier 1 Document section 3.1).

3.4.3. Recommendations

Clause 6.1.2.1 states that the following hazards are to be identified and addressed. It seems that the majority of these factors are already being considered by the City, however it would be helpful to include this list somewhere within the OHSMS to ensure that all of these hazards/risks are considered.

- How work is organised, social factors (including workload, work hours, victimisation, harassment and bullying), leadership and the culture of the organisation;

- Routine and non-routine activities and situations, including hazards arising from:
  - Infrastructure, equipment, materials, substances and the physical conditions of the workplace;
  - Produce and service design, research, development, testing, production, assembly, construction, service delivery, maintenance and disposal;
  - Human factors;
  - How the work is performed
- Past relevant incidents, internal or external to the organisation, including emergencies, and their causes;
- Potential emergency situations;
- People, including consideration of:
  - Those with access to the workplace and their activities, including workers, contractors, visitors and other persons;
  - Those in the vicinity of the workplace who can be affected by the activities of the organisation;
  - Workers at a location not under the direct control of the organisation;
- Other issues, including consideration of:
  - The design of work areas, processes, installations, machinery/equipment, operating procedures and work organisation, including their adaptation to the needs and capabilities of the workers involved;
  - Situations occurring in the vicinity of the workplace caused by work-related activities under the control of the organisation;
  - Situations not controlled by the organisation and occurring in the vicinity of the workplace that can cause injury and ill health to persons in the workplace;
- Actual or proposed changes in organisation, operations, processes, activities and the OH&S management system
- Changes in knowledge of, and information about, hazards.

3.5. Assessment of OH&S risks and other risks to the OH&S management system (6.1.2.2 - ISO 45001:2018)

3.5.1. Document Review Analysis

The City's commitment to risk and hazard identification and control are clearly established in the OHS Policy in all three Tier documents.

The risk matrix Introduced in the Tier 2 document is introduced again in the Tier 3 document. The section on hazard and risk management includes flowcharts and diagrams that explain different types of hazards and provides 5 clearly defined steps for hazard and risk control (Section 3.1 Hazard and Risk Management).

The document references the City's CRM (Customer Response Management) System as a pathway to report hazards as well as the Safety Interaction Form D20/41036* (Tier 3 document, page 24).

The Tier 3 Document includes a flowchart for the hazard and incident reporting process as well as references the document control for the Incident Report form D10/711 v* (Page 30) and Hazard Reporting form D14/75246 v* (Page 16).

3.5.1. ISO 45001:2018 Compliance Assessment

No. Although the Tier Documents talk in broad terms about risk management processes, details of how organisational-wide risks identified and managed are not included. An annual risk assessment

forum should be undertaken to ensure all risks are identified and controlled appropriately. The process for this should be documented in the OHSMS.

3.5.2. Recommendations

From review of the Risk Register, it is unclear when the last risk review was undertaken? And was this undertaken as a group workshop with workers, supervisors, managers and executives involved? It is recommended that an annual risk workshop is undertaken. It is important that there are representatives from each business unit/work area, health and safety representatives, members of the OSH committee, supervisors, managers & senior managers/executives. In preparation for this workshop, the following documentation should be gathered (& reviewed during the workshop):

- Health and Safety lead & lag indicators from previous years
- Details of previous incidents & injuries
- Details of hazards that have been reported
- Safety alerts from DMIRS etc. that may be relevant to your business.
- Legislation and relevant guidance notes, codes of practice, standards etc.
- Manuals & instructions from machinery/equipment etc etc.
  (This list is not exhaustive but just to provide an idea of what information may assist in identifying hazards/risks.)

During this workshop all attendees should be involved in brainstorming to identify hazards and risks. These hazards and risks are recorded on the risk register. The risk assessment team will then be involved in reviewing current control measures and determining whether further control measures are required & what the residual risk is and whether or not the residual risk is acceptable. This document essentially becomes the organisation's 'risk profile'. The information from the risk profile feeds down to policies, procedures, plans, SWMS etc.

3.6. Assessment of OH&S opportunities and other opportunities for the OH&S management system (6.1.2.3 - ISO 45001:2018)

3.6.1. Document Review Analysis

Key to managing organisational risks is ensuring that there are processes in place to identify all risks. If risks are not identified, they cannot be eliminated or reduced. Furthermore, the OHSMS must include an element of review, to ensure that OHS performance is continually monitored and improved upon. The OHSMS must include processes for change management. For example, a risk assessment should be undertaken before any change occurs (i.e. purchasing of new equipment, a new worker joins the team, a new project undertaken etc.).

The City's risk management processes are clearly documented in all Tier Documents. Additionally, it is evident that the City identifies risks and implements control measures for risk reduction throughout their operations (reference: Risk Register for Risk Identification – City Operations and OHS Plan).

The City's OHSMS includes various other methods to improve upon OH&S performance:

- Reporting and close out of hazards
- Management review
- SWMS
- OSH Committee

3.6.1. ISO 45001:2018 Compliance Assessment

Yes.

3.6.2. Recommendations

None.

3.7. Determination of legal requirements and other requirements (6.1.3 - ISO 45001:2018)

3.7.1. Document Review Analysis

The City's Health and Safety Policy also strongly highlights both its legislative responsibility and commitment to compliance to ensure all requirements are met.

As referenced in section 2.4 of this document, all Tier Documents have strong references to the City's responsibility under various Acts and associated legislation.

Legislation and standards are listed in various documents throughout the OHSMS. For example, OSH – Guideline- Contractor Management includes reference to legal requirements (5.3 Responsibility and Accountability).

3.7.2. ISO 45001:2018 Compliance Assessment

Yes. There are clear guidelines for the requirement of each business unit to ensure they are aware and meet their legal requirements and ensure they are kept up to date. Operations are required to ensure compliance to legal requirement when developing and reviewing the operational systems.

3.7.3. Recommendations

None.

3.8. Planning to achieve OH&S objectives (6.2.2 - ISO 45001:2018)

3.8.1. Document Review Analysis

The Tier 1 Document identifies who is responsible for assigning performance objectives (Section 2.2 Leadership and Accountability). Key performance requirements are referenced in each section of the Safety Management Plan. The Tier 2 Document has a small section 'Safety and Health Action plan' (Action Plan guidelines and considerations) which states annual health and safety KPI's are identified and set during the staff development review process.

3.8.2. ISO 45001:2018 Compliance Assessment

Yes. Actions are defined to address the OHSM objectives which are consistent with the City's Health and Safety Policy. They mention KPI's for achieving safety targets that are set during yearly review processes of the City Senior Personnel responsible for safety. There are multiple references with regards to monitoring and communicating Health and Safety Outcomes.

3.8.3. Recommendations

Does the City have a process to set KPI's for health and safety lead and lag indicators? Are these KPI's set by the executive management? How are these KPI's monitored? What happens if a business unit does not meet their KPI's? It would be beneficial to provide details of how KPI's are set and monitored in the Tier Documents.
These considerations would be satisfied with an annual management review forum.

3.9. Competence (7.2 - ISO 45001:2018)

3.9.1. Document Review Analysis

Tier 1 section 3.3 Implementation and Delivery, details the City's approach to its responsibilities with regards to education of all stakeholders. It identifies key performance requirements and details the training needs of staff, contractors, and other City stakeholders as well as the required competencies of each identified position.

Resources for training such as induction, on the job training, safe work practices and effective supervision are detailed.

Additionally, the requirement and responsibility of the City to provide resources to ensure efficient training as well as accountability for all levels of City Employees are detailed in section 3.3.

Responsibilities for each level of management are identified, from Chief Executive Officer, Directors and Managers through to Employees and Contractors. This re-enforces the City's understanding and commitment that everyone is responsible for safety at all levels within the organisation.

3.9.2. ISO 45001:2018 Compliance Assessment

Yes.

3.9.3. Recommendations

None.

3.10 Communication (7.4 - ISO 45001:2018)

3.10.1 Document Review Analysis

All key aspects of OHS communications are well defined in all Tier Documents.

Tier 1 Section 2.5 references internal and external communication requirements broadly on all Safety and Health Matters.

KPI's are set and the City demonstrates its commitment with regards to consultation of its workforce, providing platforms to identify hazards and risks and encouraging participation in review processes.

It clearly identifies the City's requirement for all employees to participate and to be actively involved in the management of hazards and risks.

Tier 2 document section 3.2 Working Alone Guidelines provides details of communication requirements for when employees are working alone.

Tier 2 document section 3.4 Change Management Standard references various processes used to communicate change to stakeholders. Emergency changes have a dedicated section to ensure immediate action needs are recognised using standard hazard / risk management practices of identifying, analysing, and controlling guidelines. This section also provides the various authority

levels and their area of responsibility with regards to approval for changes of Policy, Management Systems, Procedural and Equipment.

Tier 3 document references the importance of Safety and Health Representatives (Page 24) with regards to effective communication within the workplace.

3.10.2 ISO 45001:2018 Compliance Assessment

Yes. Procedures to ensure relevant information is communicated throughout the organisation are sufficient. The framework documentation identifies all internal and external stakeholders and how information is communicated.

3.10.3 Recommendations

None.

3.11 Emergency preparedness and response (8.2 - ISO 45001:2018)

3.11.1 Document Review Analysis

Unplanned or unexpected events require an immediate response to minimise adverse effects on the health and safety of workers and relevant interested parties such as residents, visitors, employees, contractors, and emergency services personnel.

Tier 1 Section 2.3 Emergency Management and Business Continuity provides broad guidelines to the City's commitment to ensure an Emergency Management Plan is in place and that all business units have relevant Emergency Response Plans for their area of operations. Emergency plans are required to be understood by key duty holders and are tested on a regular basis to ensure effectiveness.

Tier 2 Section 2.3 Incident Management Response provides further details on the City's emergency and business continuity plans and senior management and personnel's responsibilities are clearly defined.

Tier 2 Section 3.1 Hazard and Risk Management provides a table of responsibilities for emergency management with the Emergency Planning Committee (EPC) and Emergency Control Organisation (ECO)'s roles and responsibilities listed.

Emergency Works are referenced with guidelines on the requirements associated with performing these works including safety management plans, risk assessments, safe work method statements and job safety analysis mentioned as some of the controls to ensure safety and health requirements are met.

Emergency Changes in Tier 2 Section 3.4 provides a clear chain of responsibility for the approval of activities that may bring about change which require health and safety consideration.

Section 3.5 Training and Supervision states all employees, contractors and volunteers will be inducted in emergency procedures.

Tier 3 Emergency and Planning Section page 9 provides further details on roles and responsibilities, the scope of emergency plans. It references Australian Standard AS 3745-2010 planning for emergencies in facilities and goes into greater detail on how emergency plans are designed, implemented, communicated, tested and reviewed.

The approach is detailed and ensures all stakeholders, including facility occupants who may have a disability are catered for in the event of an emergency.

3.11.2 ISO 45001:2018 Compliance Assessment

Yes. Emergency response processes and responsibilities are clearly defined. Guidelines for testing the emergency Plans are identified and review requirements established for all business units and departments of the City.

3.11.3 Recommendations

None.

3.12 Monitoring, Measurement, Analysis and Performance Evaluation (9.1 - ISO 45001:2018)

3.12.1 Document Review Analysis

Legal Requirements:

The City's Occupational Safety and Health Policy recognises its responsibility under the WA Occupational Safety and Health Act (1984) and associated legislation.

Through all Tier documents, specific mention of various Acts and relevant legislations are made.

Tier 2 Section 6 Related Documents and Tier 3 Related Documents (Page 35) provide a comprehensive listing of Acts and relevant legislation to the development of the Safety and Health Management plan of the City.

Hazard Identification, Risk and Opportunities:
The fourth safety control pillar included in all three Tier documents specifically references Monitoring, Measurement and Evaluation.

Tier 1 defines the City's Overview of the Safety and Health program. Tier 2 defines the 'what and how' of the programme and Tier 3 further defines the 'how' of the program.

Section 4 Monitoring, Measurement and Review identifies the requirement for a culture of self-assessment, measurement, and assessment to ensure continuous improvement of the system.

Tier 2 section Hazard and Risk Management Process identifies various methods for the management of Hazards and Risks:

- Ongoing monitoring of day-to-day tasks and work areas.
- Observation and inspection.
- Use of one-off hazard/risk identification processes.
- Investigation of incidents.
- Contractors submitting work activity specific safety and health plans.
- Reviews and audits, or technical assessments of high-risk activities, areas, or processes.

As most of the City's services are provided by contractors, particular attention with regards to Contractor Management is given in section 3.3 Contractor Management which includes a number of controls required by relevant business/department heads of the City with regards to their responsibilities to measure and assess compliance.

Section 3.4 Change Management Standard identifies that analysis and audit reports are a key factor in improving the identification, control and improvement of hazards and risks.

Objectives and targets, effectiveness, and audit review frequency:
The monitoring, measurement and evaluation of the Health and Safety Plan are referenced throughout Tier 1 and 2 documents. Section 2 of Tier 1 Document provides strong emphasis on roles and responsibilities of standard and procedure implementation which pays particular attention to monitoring, audit, and management review.

Section Monitoring, Measurement and Evaluation of Tier 3 document (page 29) refences Safety Audits (LGIS 3 Steps to Safety program) to drive safety performance and claims minimisation. Annual health and safety KPI's being based around the recommendation from annual safety and health review processes.

Stakeholders' pathways are identified in section Employee Participation (page 22) where several pathways for health and safety issues can be resolved by employees, representatives and various group meetings.

3.12.2 ISO 45001:2018 Compliance Assessment

Yes. Requirements for the monitoring and measurement of legal requirements, hazard identification and control as well as monitoring and review are well defined for each of the City's responsibilities.

3.12.3 Recommendations

None.

3.13 Maintenance, calibration, or verification of monitoring equipment (9.1.1 (cont.) - ISO 45001:2018)

3.13.1 Document Review Analysis

Section 2.2 Leadership and Accountability of Tier 1 Document establishes responsibility of staff and contractors to participate in training and working safely by the proper use of safety equipment.

Section 3.1 Hazard and Risk Management sets the requirement for systems to be established with regards to procedures for maintenance, inspection, testing, calibration, and where applicable certification as required by legal and manufacturers' requirements.
Section 3.2 sets a requirement for procedures to be established, implemented, and maintained for maintenance activities to minimise safety and health risks.

The City identifies risk assessment and/or Safe Work Method Statements (SWMS) as processes to assess and control hazards/risks within the workplace. New equipment requires an approved SWMS as well as training schedule prior to purchase and implementation within the workplace.

Section 2.1 of Tier 2 Document provides guidelines for Personal Protective Equipment (PPE) maintenance.

3.13.2 ISO 45001:2018 Compliance Assessment

Yes. The roles and responsibilities of all personnel involved in ensuring legal, manufacturers and business unit's procedures are well established.

3.13.3 Recommendations

None.

3.14 Evaluation of compliance (9.1.2 – ISO 45001:2018)

3.14.1 Document Review Analysis

The way in which compliance requirements are assessed, particularly around legislative requirements, are referenced in the City's Safety and Health policy. Section 4. Monitoring, Measurement and Review provides the frequencies for the audit of the system as well as changes to compliance requirements.

A process is established for the non-compliance by Contractors in Section 3.3 Contractor Management.

3.14.2 ISO 45001:2018 Compliance Assessment

Yes.

3.14.3 Recommendations

The establishment of an annual management review forum – see below.

3.15 Internal audit program (9.2.2 – ISO 45001:2018)

3.15.1 Document Review Analysis

Tier 1 Section 4 Monitoring, Measurement and Review states that safety and health performance is monitored, audited, and reviewed periodically. A three yearly audit time frame is listed for the review of the framework and system. There are no other timeframes / frequencies mentioned in Tier 1 Document.

Audit implementation and reviews are mentioned as an important part of change management in Tier 2 Document, but no timeframes are listed as reference.

In Tier 3 Document, Section 'Monitoring, Measurement and Evaluation' (page 29), Safety Audits notes the OHS section will schedule (via Outlook calendar) notification of the requirement for a workplace inspection.

Internal Audits are mentioned in the fourth pillar of the Safety Control Pillars for the City, but there is no information with regards to frequency within business units/departments.

3.15.2 ISO 45001:2018 Compliance Assessment

Yes.

3.15.3 Recommendations

The frequency of OHSMS internal audits should be defined and documented (Tier 1 Monitoring, Audit and Management Review). It would be helpful for audit documentation to be listed in the Tier 1 document. i.e. audit criteria, audit report from etc.

3.16 Management review (9.3 – ISO 45001:2018)

3.16.1 Document Review Analysis

Section 4 Monitoring, Measurement and Review of Tier 1 Document provides a timeframe for the review of the Safety and Health Management Framework.

It is stated that Safety and Health performance is regularly measured, monitored, recorded, and analysed and reported via a mix of lead and lag performance indicators.

It is also stated that an audit of the OHSMS is conducted regularly.

3.16.2 ISO 45001:2018 Compliance Assessment

No. Although certain elements of management review are mentioned in the City's Tier Documentation, it appears that there is no formal management review of the system.

3.16.3 Recommendations

An annual management review forum would add value in ensuring that OHS objectives and targets remain relevant. It would also ensure that the OHSMS is continually improved upon.

The forum should include a combination of the following: Executive level managers, senior managers and managers. At the forum the following should be discussed to assess if there are any opportunities for improvement or if any changes are necessary:

- Results of internal audits
- Results of monitoring and measurement (i.e. KPI's)
- Evaluations of compliance with legal requirements
- Feedback/consultation (i.e. from speaking with 'shop floor' staff, was anything identified that could improve the OHSMS?)
- Communication/feedback from interested parties and stakeholders (i.e. a hazards that members of the public have reported)
- Analysing of data to identify trends that may give insight to something that needs to be changed
- Review of policy and objectives and targets (are they still relevant? Are we meeting the goals? How can they be improved upon?)
- Follow-up on previous management review actions
- Trends in incident investigations, non-conformances, corrective actions and continual improvement (i.e. are there trends or patterns? Does the same or similar risk keep occurring? How can this be improved upon?)
- Changing circumstances related to OHS (i.e. changes to WHS legislation & what this means, changes to the community, changes to any interested parties etc.)

It is recommended that the process for an annual management review forum is documented within the OHSMS. It would be helpful to develop a 'Annual Management Review Agenda' template with the above points. The forum would need to be documented (minutes of meeting) and actions assigned and closed out.

3.17 Incident, nonconformity and corrective action (10.2 – ISO 45001:2018)

3.17.1 Document Review Analysis

Tier 1 Document lists the various chains of responsibilities with regards to incident reporting and investigation. Section 3.4 Incident Management states that incidents are to be reported, investigated, and analysed to ensure appropriate corrective actions are identified and implemented. This will ensure the effectiveness and required changes are identified and procedures and other business unit tools are updated to meet the changes required.

Tier 2 Section 3.3 Incident Reporting deals with contractor safety management and reporting processes and corrective actions taken as required as well as their effectiveness.

Section 4 of Tier 2 Document, Reporting and Review satisfies requirements with regards to the summarisation of what constitutes an incident and the subsequent required actions with regards to reporting, investigating, and implementing corrective actions as required.

Tier 3 Document goes into detail with regards to injury and incident review processes. A review schedule is stated on page 31, stating reviews will occur as required with the OHS committee as well as half and yearly to identify injury trends.

3.17.1 ISO 45001:2018 Compliance Assessment

Yes. Processes for reporting incidents, investigating, identifying, and implementing corrective actions are well defined.

3.17.2 Recommendations

None.

3.18 Continual improvement (10.3 – ISO 45001:2018)

3.18.1 Document Review Analysis

Part of the introduction of the Framework of the City (Section 1.1 City of Kwinana – Safety and Health Pillars – Tier 1), within the Safety and Health Pillars sections specifically references meeting Health and Safety Targets to drive continual improvement in performance.

Section 2 Planning and Resources recognises Safety and Health Management is an integral part of business planning with specific measurement criteria to drive continual improvement in performance.

Section 2.5 Communication and Consultation states employee participation is key to achieving health and safety targets, point 4 of the employee participation section refers to employee participation in providing suggestions and solutions for the improvement of the OHSMS.

Section 4.1 of Tier 1 Document, Monitoring, Audit and Management Review assigns responsibility with management to drive continuous improvement.

Hazard and Risk Management Section of Tier 3 Document (page 26) identifies Low Risk events to be managed via continuous improvement process.

3.18.2 ISO 45001:2018 Compliance Assessment

Yes. Various processes as well as the identification of resources are present and consultation processes identified to ensure continuous improvement of the OHSM.

3.18.3 Recommendations

None.

4. Recommendations

The table below summarises the recommendations which should be made to improve the City's OHSMS. You will see that there are two clauses that the City's OHSMS does not satisfy. There are an additional six clauses that the City's OHSMS does essentially meet, however opportunities for improvement are identified. In total, there are eight specific areas in which the City's OHSMS may be improved upon. Finally, a general recommendation to improve the documents within the OHSMS is provided.

Item assessed	Complies with ISO 45001:2018	Recommendations	Priority
3.1 Determining the scope of the OH&S management system (4.3 – ISO 45001:2018)	Yes	No	N/A
3.2 OH&S Policy (5.2 – ISO 45001:2018)	Yes	No	N/A
3.3 Organisational roles, responsibilities and authorities (5.3 – ISO 45001:2018)	Yes	Yes	Low
3.4 Hazard identification (6.1.2 – ISO 45001:2018)	Yes	Yes	Medium
3.5 Assessment of OH&S risks and other risks to the OH&S management system (6.1.2.2 ISO 45001:2018)	No	Yes	High
3.6 Assessment of OH&S opportunities and other opportunities for the OH&S management system (6.1.2.3 – ISO 45001:2018)	Yes	No	N/A
3.7 Determination of legal requirements and other requirements (6.1.3 – ISO 45001:2018)	Yes	No	N/A
3.8 Planning to achieve OH&S objectives (6.2.2 – ISO 45001:2018)	Yes	Yes	Medium
3.9 Competence (7.2 – ISO 45001:2018)	Yes	No	N/A
3.10 Communication (7.4 – ISO 45001:2018)	Yes	No	N/A
3.11 Emergency preparedness and response (8.2 – ISO 45001:2018)	Yes	No	N/A
3.12 Monitoring, measurement, analysis and performance evaluation (9.1 - ISO 45001:2018)	Yes	No	N/A
3.13 Maintenance, calibration, or verification of monitoring equipment (9.1.1 (cont.) - ISO 45001:2018)	Yes	No	N/A
3.14 Evaluation of compliance (9.1.2 – ISO 45001:2018)	Yes	Yes	High
3.15 Internal audit program (9.2.2 – ISO 45001:2018)	Yes	Yes	Medium
3.16 Management review (9.3 – ISO 45001:2018)	No	Yes	High
3.17 Incident, nonconformity and corrective action (10.2 – ISO 45001:2018)	Yes	No	N/A
3.18 Continual improvement (10.3 – ISO 45001:2018)	Yes	No	N/A
The City's OHSMS would be improved by ensuring that each document provides information on the parent-child relationship.	N/A	Yes	Low

Key:

Priority	Description
High	These items are critical and should be closed out as soon as practicable (it is recommended these forums/workshops are scheduled to take place within two months).
Medium	These items are essential to an affective OHSMS and should be actioned within 3 months, if possible.
Low	These items would enhance the OHSMS and should be actioned within 6 months, if possible.

5. Audit Summary

Tier 1, 2 and 3 Documents of the City of Kwinana Safety and Health Management Framework meet most of the requirements of 45001. Opportunities for improvement have been identified, as listed in the above recommendations.

ISO 45001:2018 is based on the Annex L, the standard how ISO Management Systems should be written. ISO 45001:2018 is a quality, safety system which not only focuses on managing OHS but also provides focus on internal and external interactions within the organisational and functional procedural aspects of the organisation.

Documents within a system should link with subordinate documents and ensure readers are able to navigate within the business management systems. The inclusion of Appendices to provide further assistance in defining the framework of the OHSMS is recommended to allow greater points of references for the document users.

All Tier Documents could also benefit from additional detail of how particular outcomes will be achieved. For example, there is a requirement to identify and stay updated with legislative requirements. How is this achieved? Is there a formal group forum that business units attend to review legislative changes? Is there a person within the organisation that is responsible for identifying and communicating legislative changes? The auditor understands that the OHS Management Action Plan is currently being reviewed and updated and the City may already be in the process of adding further detail within this document.

6.2 Risk Management Reporting

SUMMARY:

Council has endorsed a Risk Management Council Policy to manage all risks that have been identified and that could impact the City if they were not managed and evaluated appropriately. At each Audit and Risk Committee Meeting, a report is presented detailing identified risks outside of the City's tolerances and the status of actions to manage those risks. Contained at Attachment A is a copy of the Camms.Risk Organisational Risk Register for noting and comment by the Committee. Contained within Confidential Attachment A and B are copies of the Camms.Risk Organisational Risk Registers for both strategic and operational risks, for noting and comment by the Committee.

The City is continuing its transitioning from spreadsheet-based risk registers to Camms.Risk software for the recording and managing of its risks. Key staff have undergone further training in relation to risk assessment and the use of Camms.Risk, in order to further strengthen the City's risk management capability.

OFFICER RECOMMENDATION:

That the Audit and Risk Committee note and provide comment where appropriate on:

- **City of Kwinana Organisational Risk Register – Strategic Risks detailed in Confidential Attachment A.**
- **City of Kwinana Organisational Risk Register – Operational Risks detailed in Confidential Attachment B.**

DISCUSSION:

The City's Risk Management Strategy sets the following role and responsibilities for the Committee:

a) Ensuring the City has appropriate risk management and internal controls in place;
b) Approving and reviewing risk management programmes and risk treatment options for extreme risks;
c) Setting and reviewing risk management tolerances/appetite and making recommendations to Council;
d) Providing guidance and governance to support significant and/or high profile elements of the risk management spectrum;
e) Monitoring strategic risk management and the adequacy of internal controls established to manage the identified risks;
f) Monitoring the City's internal control environment and reviewing the adequacy of policies, practices and procedures;
g) Assessing the adequacy of risk reporting;
h) Monitoring the internal risk audit function, including development of audit programs as well as monitoring of audit outcomes and the implementation of recommendations;
i) Setting the annual internal audit plan in conjunction with the internal auditor taking into account the City Strategic and Operational Risk Registers;
j) Conduct an annual review of the organisation's Risk Management Policy and Strategy; and
k) Reporting through the Chief Executive Officer to the Council on its findings.

6.2 RISK MANAGEMENT REPORTING

The Organisational Risk Register is provided to the Audit and Risk Committee on a quarterly basis for their review and as an opportunity to provide advice regarding risk management, as the City is focussed on creating a culture that is committed to openness and transparency and fulfilling its responsibilities in relation to risk management.

The City of Kwinana Risk Management Strategy establishes the risk appetite/attitude for residual risk as follows:

Impact Category	Level of residual risk the City is willing to retain			
	Low	Moderate	High	Extreme
Environmental		●		
Financial	●			
Health and Safety	●			
ICT, Infrastructure and Assets		●		
Legislative Compliance	●			
Reputation/Image	●			
Service Delivery		●		

The Organisational Risk Register shows all strategic risks as well as all operational risks showing a residual risk assessment of 'high' or above.

It should be noted that the register is still in relatively early stages of implementing Camms.Risk. The City recently retained Stantons to undertake training to key staff with respect to risk assessment as well as in relation to the use of Camms.Risk in a manner consistent with the City's Risk Management Strategy and Policy. Further internal training in intended to be rolled out shortly. Whilst teams across the City have yet to fully transition all previous risks into the Camm.Risk system, this remains a ongoing task and a priority for the Governance and Legal Team.

LEGAL/POLICY IMPLICATIONS:

Regulation 17 of the Local Government (Audit) Regulations 1996 provides:

17. CEO to review certain systems and procedures

(1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to —
(a) risk management; and
(b) internal control; and
(c) legislative compliance.

(2) The review may relate to any or all of the matters referred to in subregulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.

(3) The CEO is to report to the audit committee the results of that review.

6.2 RISK MANAGEMENT REPORTING

FINANCIAL/BUDGET IMPLICATIONS:

There are no financial implications identified as a result of this report.

ASSET MANAGEMENT IMPLICATIONS:

There are no asset management implications identified as a result of this report.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no direct environmental or public health implications identified as a result of this report.

STRATEGIC/SOCIAL IMPLICATIONS:

There are no strategic/social implications as a result of this proposal.

COMMUNITY ENGAGEMENT:

There are no community engagement implications as a result of this report.

6.3 Strategic Internal Audit Plan 2021/2022 to 2023/2024

SUMMARY:

The role of internal auditing is to assist the Council and senior management meet the Council's objectives by providing an independent appraisal of the adequacy and effectiveness of processes and controls. It is considered to be an essential part of achieving best practice in the management of strategic and operational risk.

Following a formal request for quotation process undertaken by the City, Paxon Group ('Paxon') were selected to prepare an internal audit plan which identifies areas to be audited across all City departments, as well as appropriate auditing hours. The plan was developed the plan on the basis of areas identified within the City's risk registers as being higher risk areas which could benefit the most from strengthening of practices.

The proposed Strategic Internal Audit Plan 2021/2022 to 2023/2024 is presented at Confidential Attachment A for consideration and comment by the Audit and Risk Committee.

OFFICER RECOMMENDATION:

That the Audit and Risk Committee review, to provide comment where necessary and refer the Strategic Internal Audit Plan 2021/2022 to 2023/2024 (as at Confidential Attachment A) to Council for adoption.

DISCUSSION:

Due to an increased focus on the accountability of local governments, a review of the effectiveness of all business processes is becoming best practice. Internal audit is one way to reduce risk and identify improvements in internal controls. There are many benefits to conducting internal audits, such as:

- improving the performance of the organisation;
- making the organisation process-dependent instead of person-dependent;
- identification of redundancies in operational and control procedures and the provision of recommendations to improve the efficiency and effectiveness of procedures;
- it serves as an early warning system, enabling deficiencies to be identified and remediated on a timely basis (i.e. prior to external, regulatory or compliance audits); and
- increases accountability within the organisation and supporting strategic objectives (for example cost reduction initiatives).

Paxon have developed a proposed Strategic Internal Audit Plan 2021/2022 to 2023/2024 detailed in Confidential Attachment A.

6.3 STRATEGIC INTERNAL AUDIT PLAN 2021/2022 TO 2023/2024

Area of Review	**2021/22 (hours)**	**2022/23 (hours)**	**2023/24 (hours)**
Planning & Building	80		
Asset Management	80		
Community Services – Events (Community Engagement, Resource Centre, Family Day Care, Events)	80		
Recquatic		80	
Environmental & Health Services/Waste		80	
Finance - Financial Management Regulation 5*		80	
Project/Program Management (Building, Operations & Engineering)		80	
Occupational Safety & Health / Human Resources			80
City Legal & Governance - Audit Regulation 17 (Legislative compliance, risk and internal control)*			80
Business Continuity/Disaster Recovery/Pandemic/Emergency Planning			80
Essential Services (Security, Rangers & Parking)			80
City Strategy			
Customer service			
Information Technology			
Contracts & Procurement	80		

Further areas identified for consideration in the current or future audit plans are as follows:

- Marketing and Communications (media and social media)
- Records/Freedom of information
- Fleet
- Grants
- Investments
- Payroll
- Asbestos and Pesticides
- Environmental/Sustainability/Green policies

LEGAL/POLICY IMPLICATIONS:

Section 7.13 of the *Local Government Act 1995* provides:

7.13. Regulations as to audits

(1) Regulations may make provision as follows —

(aa) as to the functions of a CEO in relation to —

(i) a local government audit; and

*(ii) a report (an **action report**) prepared by a local government under section 7.12A(4)(a); and*

(iii) an audit report; and

(iv) a report on an audit conducted by a local government under this Act or any other written law;

(ab) as to the functions of an audit committee, including in relation to —
(i) the selection and recommendation of an auditor under Division 2; and
(ii) a local government audit; and
(iii) an action report; and
(iv) an audit report; and
(v) a report on an audit conducted by a local government under this Act or any other written law;
(ac) as to the procedure to be followed in selecting an auditor under Division 2;
[(ad) deleted]
(ae) as to monitoring action taken in respect of any matters raised in an audit report;
*(a) with respect to matters to be included in an agreement in writing (**agreement**) made under section 7.8(1);*
(b) for notifications and reports to be given in relation to an agreement, including any variations to, or termination of an agreement;
(ba) as to a copy of an agreement being provided to the Department;
(c) as to the manner in which an application may be made to the Minister for approval as an auditor under section 7.5;
(d) in relation to approved auditors, for the following —
(i) reviews of, and reports on, the quality of audits conducted;
(ii) the withdrawal by the Minister of approval as an auditor;
(iii) applications to the State Administrative Tribunal for the review of decisions to withdraw approval;
(e) for the exercise or performance by auditors of their powers and duties under this Part;
(f) as to the matters to be addressed in an audit report;
(g) requiring an auditor (other than the Auditor General) to provide the Minister with prescribed information as to an audit conducted by the auditor;
(h) prescribing the circumstances in which an auditor (other than the Auditor General) is to be considered to have a conflict of interest and requiring an auditor (other than the Auditor General) to disclose in an audit report such information as to a possible conflict of interest as is prescribed;
(i) requiring local governments to carry out, in the prescribed manner and in a form approved by the Minister, an audit of compliance with such statutory requirements as are prescribed whether those requirements are —
(i) of a financial nature or not; or
(ii) under this Act or another written law.
(2) Regulations may also make any provision about audit committees that may be made under section 5.25 in relation to committees.

Regulation 16 of the *Local Government (Audit) Regulations 1996* provides:

16. Functions of audit committee
An audit committee has the following functions —
(a) to guide and assist the local government in carrying out —
(i) its functions under Part 6 of the Act; and
(ii) its functions relating to other audits and other matters related to financial management;
(b) to guide and assist the local government in carrying out the local government's functions in relation to audits conducted under Part 7 of the Act;

*(c) to review a report given to it by the CEO under regulation 17(3) (the **CEO's report**) and is to —*
(i) report to the council the results of that review; and
(ii) give a copy of the CEO's report to the council;
(d) to monitor and advise the CEO when the CEO is carrying out functions in relation to a review under —
(i) regulation 17(1); and
(ii) the Local Government (Financial Management) Regulations 1996 regulation 5(2)(c);
(e) to support the auditor of the local government to conduct an audit and carry out the auditor's other duties under the Act in respect of the local government;
(f) to oversee the implementation of any action that the local government —
(i) is required to take by section 7.12A(3); and
(ii) has stated it has taken or intends to take in a report prepared under section 7.12A(4)(a); and
(iii) has accepted should be taken following receipt of a report of a review conducted under regulation 17(1); and
(iv) (iv) has accepted should be taken following receipt of a report of a review conducted under the Local Government (Financial Management) Regulations 1996 regulation 5(2)(c);
(g) to perform any other function conferred on the audit committee by these regulations or another written law.

FINANCIAL/BUDGET IMPLICATIONS:

There are no direct financial implications identified as a result of this report.

ASSET MANAGEMENT IMPLICATIONS:

There are no direct asset management implications identified as a result of this report.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no direct environmental or public health implications identified as a result of this report.

STRATEGIC/SOCIAL IMPLICATIONS:

There are no direct strategic/social implications as a result of this proposal.

COMMUNITY ENGAGEMENT:

There are no direct community engagement implications as a result of this report.

6.4 Developer Contribution Payment audit and Regulation 17 audit - action updates

SUMMARY:

At its meeting of 14 June 2021, the findings of the recent Regulation 17 audit conducted by Paxon Group as well as the Developer Contribution Payment ('DCP') audit conducted by Crowe Australia were presented to the Audit and Risk Committee. Both audits contained recommendations as to areas of potential improvement to current practices. Those actions, as well as details from the relevant officers regarding the their implementation are provided for noting and comment by the Committee.

OFFICER RECOMMENDATION:

That the Audit and Risk Committee note and provide comment where appropriate on the Regulation 17 audit action report detailed in Confidential Attachment A and the Developer Contribution Payment audit action report detailed in Confidential Attachment B.

DISCUSSION:

Whilst the City has made progress towards implementing the recommended actions contained in both the Regulation 17 and DCP audit reports, the majority remain ongoing. Updates will be provided to each meeting of the Audit and Risk Committee until such time as actions are finalised.

In relation to its recording and monitoring of actions, the City in presently transitioning its reporting across the organisation:

- Strategic Community Plan and Corporate Business Plan Reporting – Previously the City stored and tracked this information in Performance Manager (Civica). Progress against actions is now being reported quarterly through spreadsheets as we progress towards tracking this information in TechOne. The first quarter for this financial year is intended to be provided to Council in October.
- Team Business Plan Reporting – Remains on hold until the transition to recording this information in TechOne.
- Opportunities for Improvement and Internal Non-Conformance Reporting – The City is transitioning from Performance Manager to Promapp, with the intention of being able to identify, investigate and action an improvement/incident, rather than just report on them.

In addition, with the DCP Report being prepared within Promapp it has been noted to log as an improvement to the summary, both a column regarding the change of date where an extension has been required and the reasoning for it.

The City's IT Department are currently progressing implementing a Cyber Security Manual which will address a number of the outstanding actions relating to their area. The Cyber Security Manual is approximately 90% complete. The manual is comprehensive and takes a pragmatic approach to Cyber Security. A cyber awareness system is being implemented to provide cyber awareness testing, training and reporting on an ongoing basis.

6.4 DEVELOPER CONTRIBUTION PAYMENT AUDIT AND REGULATION 17 AUDIT - ACTION UPDATES

The schedule being implemented will sending phishing test emails monthly, training quarterly and a cyber security skill assessment annually. A baseline phishing test is scheduled for first week of October 2021.

LEGAL/POLICY IMPLICATIONS:

Regulation 17 of the Local Government (Audit) Regulations 1996 provides:

17. CEO to review certain systems and procedures

(1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to —
(a) risk management; and
(b) internal control; and
(c) legislative compliance.

(2) The review may relate to any or all of the matters referred to in subregulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.

(3) The CEO is to report to the audit committee the results of that review.

FINANCIAL/BUDGET IMPLICATIONS:

There are no direct financial implications identified as a result of this report.

ASSET MANAGEMENT IMPLICATIONS:

There are no direct asset management implications identified as a result of this report.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no direct environmental or public health implications identified as a result of this report.

STRATEGIC/SOCIAL IMPLICATIONS:

There are no direct strategic/social implications as a result of this proposal.

COMMUNITY ENGAGEMENT:

There are no direct community engagement implications as a result of this report.

6.5 2020/2021 Interim Financial Audit

SUMMARY:

The purpose of this report is to provide the Audit Committee with an overview of the 2020/2021 Interim Audit as performed by the Office of the Auditor General's contractor, RSM. The Office of the Auditor General is responsible for issuing the Interim Audit Management Letter to the City.

OFFICER RECOMMENDATION:

That the Audit Committee notes the findings of the Office of Auditor General, and Management responses to the findings, as part of the interim 2020/2021 financial and information systems audit, as detailed in Attachment A and B.

DISCUSSION:

As part of the 2020/2021 financial audit, the Office of the Auditor General (OAG) contracted RSM to perform an interim audit during May 2021. There is no requirement for Auditors to form an opinion or to produce a report as a result of an interim audit, however, the following matters have been included within the Interim Audit Management Letter. Officers have provided comments for each item for reporting to the Audit Committee with further information provided within the Interim Audit Management Letter as contained in Attachment A and B.

Auditor Note	Officer Comments
Finding: During the interim audit RSM noted infrastructure assets under construction were capitalised in the fixed asset register at year end irrespective of the constructed assets 'practical completion' date or 'in use' date. Rating: Minor Recommendation: The City should develop a policy to ensure capital works projects are regularly reviewed and capitalised as and when they're completed.	The City has recently updated the 'Recognition and Depreciation of Assets' policy as adopted by Council (OCM 14/7/2021). The Policy now includes a paragraph to clarify the treatment of Assets under Construction. Both the Assistant Accountant and Coordinator Finance frequently attend Project Management Meetings with the Engineering and Asset Management Teams to ensure they keep up to date with capital project progression. The Project Tracking meeting minutes are to be used to identify projects that can potentially by capitalised throughout the year. Due to the timing of receiving invoices some projects are unable to be closed out at the time of completion. Where possible, project commissioning will be back dated in our system to ensure the appropriate amount of depreciation is expensed during the year.

6.5 2020/2021 INTERIM FINANCIAL AUDIT

The final audit of the Annual Financial Statements for the year ended 30 June 2021 will be conducted by the OAG's contractor, RSM, during the week beginning October 4 2021. The final audit report will be issued by the OAG upon completion of the audit.

In addition to the interim financial audit, the Office of the Auditor General also completed an interim information systems audit. There were seven findings from this audit, although only one of these findings is new. The remainder are outstanding or updated findings from the 2019/2020 information systems audit. As noted in the summary table below, the previous audit findings will be addressed as part of an overall approach to the management of information technology within the City: a new information technology and communications strategic plan and Cyber Security Policy Manual. It is relevant that there is a significant amount of work in developing the strategy and manual, and the interim audit commenced less than three months after the finalisation of the 2019-2020 audit, so it is expected that these items will still be outstanding.

New Finding	
Auditor Note	**Officer Comments**
Network Security Management Finding: Noted that the City have not performed full network security/penetration testing since 2018 to understand the City's network security posture and identify any potential security weaknesses or vulnerabilities to the network. Rating: Moderate Recommendation: The City should establish a process to perform cyclical security/penetration testing on a regular basis on critical infrastructure and systems to improve network security and provide protection against any potential vulnerabilities or cyber breaches.	The finding is accepted. Penetration testing will be performed in the second quarter 2022 once remediation of the outstanding OAG findings has taken place. Completion Date: June 2022

Outstanding Finding	
Auditor Note	**Officer Comments**
IT Governance – Policies and Procedures Finding: the 'Acceptable Use of IT Systems' policy has not been reviewed since November 2007 and there were no formal policies and procedures for the following key IT functional areas: • Information security, objectives, principles, responsibilities and compliance requirements; • Incident management (Handling of security breaches and or inappropriate use); • System and user password requirements and configuration;	The finding is accepted. A new ICT Strategic Plan will be developed. Formally documented ICT governance policies and standards will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings. The network diagram is being updated to reflect the current architecture. Completion Date: December 2021: Cyber Security Policy and Manual June 2022: ICT Strategic Plan

6.5 2020/2021 INTERIM FINANCIAL AUDIT

• Protection from malware and malicious code; • User access / remote access / wireless networks management (Granting / revoking access to systems); • Review and monitoring of user access / System audit logging and monitoring; • Restrictions on software user and installations; • Mobile device management / Data loss prevention management; • Information system back-up and recovery; • IT asset management and disposal; • the City's network diagram is not periodically reviewed to ensure the diagram accurately reflect the City's current network architecture; and • the City's IT Strategy (2016 to 2020) has not been reviewed and updated to be aligned to the City's business strategy for the current and future financial years. Rating: Significant Recommendation: IT policies and procedures should be regularly reviewed, updated and communicated to users of the IT systems. They should also reflect the current network architecture and IT Strategy.	
<u>User Access Management</u> Finding: Noted the following deficiencies with the City's network access management process: • periodic user access reviews for active network administrator and user accounts are not performed**;** • 56 out of 407 active users have not logged into the systems in the last 6 months; • 1 system user of Civica Authority has system administrative privileges assigned to them which is not in line with their role and level of responsibility; and • 3 network accounts were inappropriately assigned domain privileged / administrative access.	The City reviews all user accounts regularly, although without a formalised process. User account access is reviewed for all users in the following situations: 1. when they are created; 2. if the user's role or PD is adjusted; 3. if the user relocates office or workstation; 4. if a user's direct report changes; and 5. when their employment is terminated. All network user accounts are created on request of the City's HR department, or via the new staff member's line manager. These requests are lodged formally via the IT helpdesk, and formal approval is accepted as given where the requester is someone with the authority to give the approval makes the request (i.e. line manager or Human Resources as part of the 'on-boarding' process).

6.5 2020/2021 INTERIM FINANCIAL AUDIT

Additional Findings: evidence of periodic user access reviews for domain administrator and privileged access in Civia Authority is not retained; • 22 out of 106 active user accounts have not logged into the network in the last 6 months; and • 20 out of 106 active user accounts have never logged into the network. Rating: Significant Recommendation: The City should regularly review and monitor user access to the network and Civica Authority database to ensure it is in line with employee roles and levels of responsibility. Evidence of these reviews should be retained and inactive accounts should be removed or disabled.	The City will review its current position in regards to formal review of user accounts when developing the user access policy/guideline as part of its new Strategic IT Plan. The City acknowledges that network service accounts are not formally requested or approved. However, the City has reviewed all network accounts with domain administration privileges and is satisfied that these accounts have the appropriate permissions for their purpose, and the appropriate controls are in place to ensure the integrity of the system. Further Comments: Formally documented IT governance policies and standards for network user account management standards will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings. Completion Date: December 2021
<u>Business Continuity</u> Finding: During the audit we noted there was no evidence to support the City's Disaster Recovery Plan (DRP) had been reviewed since January 2018. We also noted the City did not IT disaster recovery tests Rating: Moderate Recommendation: The City should review and update IT DRP documents. In addition to this the IT DRP should be regularly tested and the results of these tests should be recorded. The IT DRP tests should be used to confirm key IT systems and services can be recovered and data backups can be restored in accordance with the agreed recovery requirements.	The City's current IT Backup and DR Plan is reviewed annually, and was last reviewed in May 2019. It is acknowledged that the version control within the document is not up to date, and the City accepts that this is a required improvement. This plan also is reviewed on any major changes to the backup and DR systems, of which there has been none for approximately 3 years. The City considers the failure to update the version log to represent a minor finding, which will be addressed upon the next review of this plan. Updated Comment: The IT Backup and DR plan and processes will be updated as part of deploying an IT Cloud hosted DR/BCP solution and as part of the Cyber Security Policy, Manual and ICT Strategy. Documented DR/BCP testing will take place for a minimum of one business system. Completion Date: December 2021

6.5 2020/2021 INTERIM FINANCIAL AUDIT

IT Change Management Procedures Finding: The City does not have a formal system for change management procedures to ensure IT infrastructure changes are formally documented, appropriately requested, reviewed, approved and analysed. Rating: Moderate Recommendation: The City should implement formal change management controls, policies and processes to ensure changes do not compromise security, integrity of data and availability of systems. User access testing, stress tests and post implementation reviews should be implemented and documented as and when required.	Formally documented IT governance policies and standards for change management will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings. Completion Date: December 2021
<u>Physical and Environmental Security</u> Finding: Several deficiencies in the physical and environmental security management of the datacentre located at the City were noted. We noted there was no documented and approved policy or procedure to outline physical and environmental requirements for data locations, access management, and monitoring of environmental controls. Rating: Moderate Recommendation: The City should develop a policy and implement a process to ensure physical and environment security of the datacentre. Any inappropriate or unauthorised access and critical hardware failures should be investigated and action should be taken immediately to address weaknesses.	The lack of formally documented IT governance policies and standards for physical and environmental security will be addressed by a Cyber Security Policy and Manual that is currently being developed. Physical/environmental security controls will be implemented where appropriate. Completion Date: June 2022

6.5 2020/2021 INTERIM FINANCIAL AUDIT

Network Password Management Findings: We noted the City does not have a formal policy in place to enforce strong password settings within the organisation. Password parameters configured in City's network (active directory) are not aligned with better practice guidelines. Rating: Moderate Recommendation: The City should develop, document and implement a formal password management policy and ensure it aligns to better practice guidelines.	The password parameters in the better practice guidelines have been implemented. Formally documented IT governance policies and standards for password management will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings. Completion Date: Recommendation has been implemented. Additional Password Controls: December 2021

LEGAL/POLICY IMPLICATIONS:

Local Government Act 1995 section 7.12AB. states:

Conducting a financial audit
The auditor must audit the accounts and annual financial report of a local government at least once in respect of each financial year.

FINANCIAL/BUDGET IMPLICATIONS:

There are no specific financial/budget implications as a result of this report.

ASSET MANAGEMENT IMPLICATIONS:

There are no specific asset management implications as a result of this report.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no implications on any determinants of health as a result of this report.

STRATEGIC/SOCIAL IMPLICATIONS:

This proposal will support the achievement of the following outcome and objective detailed in the Strategic Community Plan and Corporate Business Plan.

Plan	Outcome	Objective
Corporate Business Plan	Visionary leadership dedicated to acting for its community	5.1 Model accountable and ethical governance, strengthening trust with the community.

COMMUNITY ENGAGEMENT:

There are no community engagement implications as a result of this report.

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

INDEX OF FINDINGS	RATING		
	Significant	**Moderate**	**Minor**
1. Capitalisation of work in progress			✓

KEY TO RATINGS

The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

Significant - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly. A significant rating may be reported as a matter of non-compliance in the audit report in the current year, or in a subsequent reporting period if not addressed. However, even if the issue is not likely to impact the audit report, it should be addressed promptly.

Moderate - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.

Minor - Those findings that are not of primary concern but still warrant action being taken.

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

1. Capitalisation of work in progress

Finding
During the interim audit we noted infrastructure assets under construction were capitalised in the fixed asset register at year-end irrespective of the constructed asset's 'practical completion date' or 'in use' date.

Rating: Minor
Implication
The City has an increased risk of incorrect asset capitalisation resulting in an overstatement of capital works in progress and understatement of fixed assets and depreciation.

Recommendation
The City should develop a policy to ensure capital works projects are regularly reviewed and capitalised as and when they're completed.

Management Comment
The City has recently updated our 'Recognition and Depreciation of Assets' policy to be adopted by Council (Council meeting to be held 14th July). This Policy now includes a paragraph to clarify the treatment of Assets under Construction.

Both the Assistant Accountant and Coordinator Finance frequently attend Project Management meetings with the Engineering and Asset Management teams to ensure they keep up to date with capital project progression. The Project Tracking meeting minutes are to be used to identify projects that can potentially be capitalised throughout the year.

Due to the timing of receiving invoices (for example, many line-marking invoices are not received until year end), some projects are unable to be closed out at the time of practical completion or 'in use' as the expenditure has not been entered into the system. However, all project commissioning, regardless of timing of creating the addition in our system, will be back dated to the notified project completion date to ensure the appropriate amount of depreciation is expensed during the year.

Responsible Person: *Vina Chang, Vikki Lauritsen*
Completion Date: *June 2021*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

INDEX OF FINDINGS	RATING		
	Significant	**Moderate**	**Minor**
1. Network Security Management		✓	
Matters outstanding from prior year audit			
2. IT Governance – policies and procedures	✓		
3. User access management	✓		
4. Business continuity		✓	
5. IT change management procedures		✓	
6. Physical and environmental security		✓	
7. Network password management		✓	

KEY TO RATINGS

The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

Significant - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly. A significant rating may be reported as a matter of non-compliance in the audit report in the current year, or in a subsequent reporting period if not addressed. However, even if the issue is not likely to impact the audit report, it should be addressed promptly.

Moderate - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.

Minor - Those findings that are not of primary concern but still warrant action being taken.

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

1. Network security management

Finding
We noted that the City have not performed full network security/penetration testing since 2018 to understand the City's network security posture and identify any potential security weaknesses or vulnerabilities to the network.

Rating: Moderate
Implication
Without regular security/penetration testing, the network and systems may become susceptible to potential security breaches and future attacks.

Recommendation
The City should establish a process to perform cyclical security/penetration testing on a regular basis on critical infrastructure and systems to improve network security and provide protection against any potential vulnerabilities or cyber breaches.

Management Comment
The finding is accepted. Penetration testing will be performed in the second quarter 2022 once remediation of the outstanding OAG findings has taken place.

Responsible Person: *Manager Information Technology (new incumbent)*
Completion Date: *30 June 2022*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

2. IT governance – policies and procedures

2020 Finding
When reviewing the City's IT policies and procedures we identified the 'Acceptable Use of IT Systems' policy has not been reviewed since November 2007 and there were no formal policies and procedures for the following key IT functional areas:

- Information security, objectives, principles, responsibilities and compliance requirements;
- Incident management (Handling of security breaches and or inappropriate use);
- System and user password requirements and configuration;
- Protection from malware and malicious code;
- User access / remote access / wireless networks management (Granting / revoking access to systems);
- Review and monitoring of user access / System audit logging and monitoring;
- Restrictions on software user and installations;
- Mobile device management / Data loss prevention management;
- Information system back-up and recovery; and
- IT asset management and disposal.

2021 Status
The 2020 finding remains unresolved. In addition to this we noted the following:

- the City's network diagram is not periodically reviewed to ensure the diagram accurately reflect the City's current network architecture; and
- the City's IT Strategy (2016 to 2020) has not been reviewed and updated to be aligned to the City's business strategy for the current and future financial years.

Rating: Significant (2020: Significant)
Implication
A lack of current IT policies and procedures consistent with the City's current network architecture and IT Strategy may result in inconsistent or inappropriate approaches being adopted by staff or contractors. This may result in security or other exposures.

Recommendation
IT policies and procedures should be regularly reviewed, updated and communicated to users of the IT systems. They should also reflect the current network architecture and IT Strategy.

2020 Management Comment
The City acknowledges and is aware that formal documentation of many of its IT policies and procedures is required, and has already begun authoring many of these for inclusion into a new Strategic IT Plan based on ISO 27001:2015 standards. This new plan will be formally adopted by the Executive Team and will be reviewed on an annual and as-needed basis.

The City's existing IT Backup and DR plan does contain some procedures and guidelines on information system back-up and recovery, and will be further developed with much more specific information.

The City's 'Acceptable use of IT Systems' policy was formally reviewed on 27th June 2018 as reflected by our Document Management System, however, the version control on the document itself does require an update.

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
A new ICT Strategic Plan will be developed. Formally documented ICT governance policies and standards will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings. The network diagram is being updated to reflect the current architecture.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *31 December 2021: Cyber Security Policy and Manual*
30 June 2022: ICT Strategic Plan

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

3. User access management

2020 Finding
We noted the following deficiencies with the City's network access management process:

- periodic user access reviews for active network administrator and user accounts are not performed**;**
- 56 out of 407 active users have not logged into the systems in the last 6 months;
- 1 system user of Civica Authority has system administrative privileges assigned to them which is not in line with their role and level of responsibility; and
- 3 network accounts were inappropriately assigned domain privileged / administrative access.

2021 Status
We noted the following deficiencies with the City's network access management process:

- evidence of periodic user access reviews for domain administrator and privileged access in Civia Authority is not retained;
- 22 out of 106 active user accounts have not logged into the network in the last 6 months; and
- 20 out of 106 active user accounts have never logged into the network.

Rating: Significant (2020: Significant)
Implication
Without appropriate user access management controls in place there is an increased risk of inappropriate or unauthorised access to the City's IT systems and/or information. This could impact the confidentiality, integrity and availability of City information.

Recommendation
The City should regularly review and monitor user access to the network and Civica Authority database to ensure it is in line with employee roles and levels of responsibility. Evidence of these reviews should be retained and inactive accounts should be removed or disabled.

2020 Management Comment
The City reviews all user accounts regularly, although without a formalised process. User account access is reviewed for all users in the following situations:

1. *when they are created;*
2. *if the user's role or PD is adjusted;*
3. *if the user relocates office or workstation;*
4. *if a user's direct report changes; and*
5. *when their employment is terminated.*

All network user accounts are created on request of the City's HR department, or via the new staff member's line manager. These requests are lodged formally via the IT helpdesk, and formal approval is accepted as given where the requester is someone with the authority to give the approval makes the request (i.e. line manager or Human Resources as part of the 'on-boarding' process). The City will review its current position in regards to formal review of user accounts when developing the user access policy/guideline as part of its new Strategic IT Plan.

The City acknowledges that network service accounts are not formally requested or approved. However, the City has reviewed all network accounts with domain administration privileges and

is satisfied that these accounts have the appropriate permissions for their purpose, and the appropriate controls are in place to ensure the integrity of the system.

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
Formally documented IT governance policies and standards for network user account management standards will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *31 December 2021*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

4. Business continuity

2020 Finding
During the audit we noted there was no evidence to support the City's Disaster Recovery Plan (DRP) had been reviewed since January 2018. We also noted the City did not IT disaster recovery tests

2021 Status
The 2020 finding remains unresolved.

Rating: Moderate (2020: Moderate)
Implication
Without an up to date IT DRP there is an increased risk that critical business functions and processes may not be appropriately recovered or restored following a major incident.

Recommendation
The City should review and update IT DRP documents. In addition to this the IT DRP should be regularly tested and the results of these tests should be recorded. The IT DRP tests should be used to confirm key IT systems and services can be recovered and data backups can be restored in accordance with the agreed recovery requirements.

2020 Management Comment
The City's current IT Backup and DR Plan is reviewed annually, and was last reviewed in May 2019. It is acknowledged that the version control within the document is not up to date, and the City accepts that this is a required improvement. This plan also is reviewed on any major changes to the backup and DR systems, of which there has been none for approximately 3 years. The City considers the failure to update the version log to represent a minor finding, which will be addressed upon the next review of this plan.

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
The IT Backup and DR plan and processes will be updated as part of deploying an IT Cloud hosted DR/BCP solution and as part of the Cyber Security Policy, Manual and ICT Strategy. Documented DR/BCP testing will take place for a minimum of one business system.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *31 December 2021*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

5. IT change management procedures

2020 Finding
The City does not have a formal system for change management procedures to ensure IT infrastructure changes are formally documented, appropriately requested, reviewed, approved and analysed.

2021 Status
The 2020 finding remains unresolved.

Rating: Moderate (2020: Moderate)
Implication
There is an increased risk that changes to the network and applications, including those that may be harmful to systems and information could be implemented without proper assessment and approval. If changes are not controlled, security and availability of systems may be compromised.

Recommendation
The City should implement formal change management controls, policies and processes to ensure changes do not compromise security, integrity of data and availability of systems. User access testing, stress tests and post implementation reviews should be implemented and documented as and when required.

2020 Management Comment
The City accepts this finding. With the exception of IT projects – no formal system for change management is in place for 'business as usual' changes to IT systems. The City will determine the need/urgency of a varying degree of formal systems and include any new change management practice in the new Strategic IT Plan.

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
Formally documented IT governance policies and standards for change management will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *31 December 2021*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

6. Physical and environmental security

2020 Finding
Several deficiencies in the physical and environmental security management of the datacentre located at the City were noted. We noted there was no documented and approved policy or procedure to outline physical and environmental requirements for data locations, access management, and monitoring of environmental controls.

2021 Status
The 2020 finding remains unresolved.

Rating: Moderate (2020: Moderate)
Implication
Without appropriate controls in place to manage the physical and environmental controls, there is an increased risk of inappropriate, unauthorised access and potential failure of critical hardware to support key infrastructure or systems. This could impact the confidentiality, integrity and availability of the City's systems and information.

Recommendation
The City should develop a policy and implement a process to ensure physical and environment security of the datacentre. Any inappropriate or unauthorised access and critical hardware failures should be investigated and action should be taken immediately to address weaknesses.

2020 Management Comment
The City acknowledges that there are opportunities for improvement in regards to security and environmental documentation. However, the City notes that controls and monitoring are in place. As an example, the City uses dual air conditioners to ensure redundancy in the environment control system, and has temperature sensors located with the City's servers, to ensure the IT team is notified in the case of total failure of the air-conditioning system.

The City does conduct regular fire and earthquake drills and disputes this finding. The City acknowledges the need to improve documentation of the procedures for and occurrence of fire and earthquake drills.

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
The lack of formally documented IT governance policies and standards for physical and environmental security will be addressed by a Cyber Security Policy and Manual that is currently being developed. Physical/environmental security controls will be implemented where appropriate.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *30 June 2022*

CITY OF KWINANA

PERIOD OF AUDIT: 1 JULY 2020 TO 30 JUNE 2021

FINDINGS IDENTIFIED DURING THE INFORMATION SYSTEMS AUDIT

7. Network password management

2020 Finding
We noted the City does not have a formal policy in place to enforce strong password settings within the organisation. Password parameters configured in City's network (active directory) are not aligned with better practice guidelines (see below):

Password Details	City Network Settings	Better Practice Guidelines
History	4	10 or more
Lockout Duration	Not defined	at least 30 mins
Lockout Threshold	Not defined	at least 5 attempts

2021 Status
The 2020 finding remains unresolved. In addition to this we note the account lockout functionality is disabled.

Rating: Moderate (2020: Moderate)
Implication
Without adequate password management protocols and procedures, there is an increased risk of unauthorised access or compromises to network and system security. The network and systems may become susceptible to potential security breaches, such as brute force or social engineering attacks.

Recommendation
The City should develop, document and implement a formal password management policy and ensure it aligns to better practice guidelines.

2020 Management Comment
The City will develop a formal policy to enforce formal passwords, as part of the review of the Strategic IT Plan.

2020 Responsible Person: *Manager Information Technology*
2020 Completion Date: *26 October 2020*

2021 Management Comment
The password parameters listed above have been implemented. Formally documented IT governance policies and standards for password management will be addressed by a Cyber Security Policy and Manual that is currently being developed. Where appropriate, processes and controls will be implemented to address these findings.

2021 Responsible Person: *Manager Information Technology (new incumbent)*
2021 Completion Date: *31 December 2021*

6.6 Review of Audit and Risk Committee Terms of Reference

SUMMARY:

The Audit and Risk Committee (Committee) Terms of Reference provides clear guidance on the purpose of the Committee and the duties and responsibilities of the Committee members.

With the upcoming Local Government Election, a review of the Terms of Reference has been undertaken, with several amendments being identified.

Following the review and approval of the Audit and Risk Committee the Terms of reference will be presented to Council for their review and adoption.

OFFICER RECOMMENDATION:

That the Audit and Risk Committee:

1. **note the amended Audit and Risk Committee Terms of Reference, as at Attachment A and provide comment where necessary; and**
2. **recommend that Council adopt the amended Audit and Risk Committee Terms of Reference, as at Attachment A.**

DISCUSSION:

A review of the Terms of Reference has been undertaken and is now recommended for Committee noting and Council adoption.

Clarification has been included with regards to the Committee not having executive powers or authority to implement actions in areas over which the Chief Executive Officer (CEO) has legislative responsibility and does not have any delegated power from Council. In addition, the Committee does not have any management functions and cannot involve itself in management processes or procedures.

Previously, the Terms of Reference referenced independent members being appointed for three year terms and Elected Members four year terms, this has been amended to be two year terms for both independent members and Elected Members to coincide with the City's ordinary election cycle and in compliance with s 5.11 of the *Local Government Act 1995*.

An amendment was also made in regards to the Committee appointment of a Chairperson, the amendment is in accordance with s 5.12 of the *Local Government Act 1995*, which prescribes that committee presiding members and deputy presiding members, must be elected in accordance with the procedures established in Schedule 2.3 of the *Local Government Act 1995*. Therefore, an election process is necessary and not a vote / resolution by the committee.

Additional minor amendments have also been made, the proposed amendments are highlighted in tracked changes within the Terms of Reference (Attachment A).

6.6 REVIEW OF AUDIT AND RISK COMMITTEE TERMS OF REFERENCE

LEGAL/POLICY IMPLICATIONS:

Local Government Act 1995:

7.1A. Audit committee

(1) A local government is to establish an audit committee of 3 or more persons to exercise the powers and discharge the duties conferred on it.

(2) The members of the audit committee of a local government are to be appointed by the local government and at least 3 of the members, and the majority of the members, are to be council members.*

** Absolute majority required.*

(3) A CEO is not to be a member of an audit committee and may not nominate a person to be a member of an audit committee or have a person to represent the CEO as a member of an audit committee.

(4) An employee is not to be a member of an audit committee.

Section 5.11

5.11. Committee membership, tenure of

(1) Where a person is appointed as a member of a committee under section 5.10(4) or (5), the person's membership of the committee continues until —
(a) the person no longer holds the office by virtue of which the person became a member, or is no longer the CEO, or the CEO's representative, as the case may be; or
(b) the person resigns from membership of the committee; or
(c) the committee is disbanded; or
(d) the next ordinary elections day, whichever happens first.

(2) Where a person is appointed as a member of a committee other than under section 5.10(4) or (5), the person's membership of the committee continues until —

(a) the term of the person's appointment as a committee member expires; or
(b) the local government removes the person from the office of committee member or the office of committee member otherwise becomes vacant; or
(c) the committee is disbanded; or
(d) the next ordinary elections day, whichever happens first.

5.12. Presiding members and deputies, election of
(1) The members of a committee are to elect a presiding member from amongst themselves in accordance with Schedule 2.3, Division 1 as if the references in that Schedule —
(a) to "office" were references to "office of presiding member"; and
(b) to "council" were references to "committee"; and
(c) to "councillors" were references to "committee members".

(2) The members of a committee may elect a deputy presiding member from amongst themselves but any such election is to be in accordance with Schedule 2.3, Division 2 as if the references in that Schedule —
(a) to "office" were references to "office of deputy presiding member"; and
(b) to "council" were references to "committee"; and
(c) to "councillors" were references to "committee members"; and
(d) to "mayor or president" were references to "presiding member".

Local Government (Audit) Regulations 1996:

16. Audit committee, functions of An audit committee —

(a) is to provide guidance and assistance to the local government —
(i) as to the carrying out of its functions in relation to audits carried out under Part 7 of the Act; and

(ii) as to the development of a process to be used to select and appoint a person to be an auditor; and

(b) may provide guidance and assistance to the local government as to —
(i) matters to be audited; and

(ii) the scope of audits; and

(iii) its functions under Part 6 of the Act; and

(iv) the carrying out of its functions relating to other audits and other matters related to financial management; and

(c) is to review a report given to it by the CEO under regulation 17(3) (the CEO's report) and is to —
(i) report to the council the results of that review; and

(ii) give a copy of the CEO's report to the council.

FINANCIAL/BUDGET IMPLICATIONS:

There are no financial/budget implications that have been identified as a result of this report or recommendation.

ASSET MANAGEMENT IMPLICATIONS:

There are no asset management implications that have been identified as a result of this report or recommendation.

ENVIRONMENTAL/PUBLIC HEALTH IMPLICATIONS:

There are no environmental/public health implications that have been identified as a result of this report or recommendation.

6.6 REVIEW OF AUDIT AND RISK COMMITTEE TERMS OF REFERENCE

STRATEGIC/SOCIAL IMPLICATIONS:

There are no strategic/social implications as a result of this proposal.

COMMUNITY ENGAGEMENT:

There are no community engagement implications as a result of this report.

ATTACHMENT A

Audit and Risk Committee - Terms of Reference

Purpose

1.1 To assist the Council to discharge its responsibility ~~to~~ with regard to the exercise of due care, diligence and skill in relation to the oversight of:

- the robustness of the internal control framework;
- the integrity and appropriateness of external reporting, and accountability arrangements within the organisation for these functions;
- the robustness of internal risk management systems, including the City's processes, practices and procedures;
- internal and external audit;
- accounting policy and practice;
- significant projects and programs of work focusing on the appropriate management of risk;
- compliance with applicable laws, regulations, standards and best practice guidelines for public entities;
- the establishment and maintenance of controls to safeguard the Council's financial and non-financial assets; and
- Councils risk appetite and the acceptability of level of risk.

The Audit and Risk Committee (Committee) is a formally appointed Committee of Council and is responsible to that body. The Committee does not have executive powers or authority to implement actions in areas over which the Chief Executive Officer (CEO) has legislative responsibility and does not have any delegated power from Council. The Committee does not have any management functions and cannot involve itself in management processes or procedures.

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 1 cm

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

1.2 As reflected in this Terms of Reference, the foundations on which this Committee operates includes: independence; clarity of purpose; competence; open, effective and respectful relationships and a transparent "no surprises" ethos.

Membership and participation

1.3 Members of the Audit and Risk Committee shall be impartial and independent at all times.

1.4 The Committee will comprise of six members, namely two independent external members and four City of Kwinana Elected Members, ~~one~~ of ~~whom~~ which should ~~be~~ include the ~~presiding~~ Mayor.

1.5 Appointment of independent members

- Identify skills required for independent members of the ~~Audit and Risk~~ Committee. Appointment panels will include the Mayor and/or Deputy Mayor and two other Elected Members. Council approval is required for all independent member appointments;
- The independent members are appointed for ~~three~~ two year terms to coincide with the City's ordinary election cycle and in compliance with section 5.11 of the *Local Government Act 1995*.
- An independent member is not to be a staff member or Elected Member.~~;~~
- Independent members are eligible for re-appointment to a maximum of two terms. By exception, the Council may approve ~~a third~~ further terms to ensure continuity of knowledge;
- The Committee will comprise of six members, namely two independent external members and four City of Kwinana Elected Members.

1.6 All Committee members have full voting rights.

1.7 The term of an Elected Member ~~Councillor's~~ appointed to the ~~c~~Committee will be for a two year term, to coincide with the City's ordinary election cycle and in compliance with section 5.11 of the *Local Government Act 1995*. ~~nd when~~ Elected Members are able to nominate/re-nominate at a meeting of Council following the ordinary election, if necessary a ballot will be conducted~~their four year term of office ceases. If the Councillor nominates for re-election to Council at the Local Government, they may be eligible to apply for re-appointment to the committee for a further term should they be successfully elected to Council following the Local Government elections.~~

~~1.8 Other than the presiding Mayor, Councillors are to serve no more than two terms on the committee.~~

~~1.9~~1.8 The Chief Executive Officer and Executive Leadership Team (herein referred to as "Management") will not be members of the Committee. The Chief Executive Officer should attend every Committee meeting and shall play a key role on the committee by providing expert advice to the Committee.

~~1.10~~1.9 The members, taken collectively, will have a broad range of skills and experience relevant to the operations of the Council. At least one ~~external~~ independent member should have accounting or related financial management experience, with an understanding of accounting and auditing standards in a public sector/local government environment.

The City recommends that o~~O~~ne of the independent members of the ~~Audit and Risk~~ Committee ~~shall~~ be appointed Chairperson ~~of the Committee~~. Section 5.12 of the *Local Government Act 1995* prescribes that committee presiding members and deputy presiding members, must be elected in accordance with the procedures established in Schedule 2.3 of the *Local Government Act 1995*. This is an election process and not a vote / resolution by the committee.

Formatted: Font: (Default) Arial, 11 pt
Formatted: Font: (Default) Arial, 11 pt
Formatted: Font: Italic
Formatted: Font: (Default) Arial, 11 pt
Formatted: Font color: Auto, Not Highlight
Formatted: Font: Italic
Formatted: Font: (Default) Arial, 11 pt
Formatted: Font: (Default) Arial, 11 pt
Formatted: Font: Italic
Formatted: Font: Not Bold

Quorum

~~1.11~~1.10 A quorum shall consist of at least 50% of the number of members of the Committee, one of whom is to be an independent member, unless a reduction is approved by the local government under s5.15 of the *Local Government Act 1995*.

Meetings

~~1.12~~1.11 The Committee should meet at times during the year that most effectively coincides with the requirements of the legislation for that year, and operational activities, with a view to providing the necessary reports well before the due dates.

Procedure

1.14 In order to give effect to its advice, the Committee should make recommendations to the Council and to Management.

~~1.15 Each meeting agenda is to include an opportunity for an in camera meeting between the Committee and the internal and the external auditors (without Management present). An in camera meeting can be held at any time during the meeting if requested by any of the Committee members present.~~

~~1.16~~1.15 The external auditors, the internal audit manager and the co-sourced internal audit firm (if appointed) should meet with the Committee Chair outside of formal meetings as considered appropriate.

~~1.17~~1.16 Where necessary, ~~T~~the Committee Chair will meet with the CEO or delegate before each Committee meeting and at other times as required as agreed by the Chair.

Duties and responsibilities

~~1.18~~1.17 Internal control framework

- Consider the adequacy and effectiveness of internal controls and the internal control framework including overseeing privacy and cyber security;
- Critically examine the steps Management has taken to embed a culture that is committed to probity and ethical behaviour;
- Review the organisation's processes or systems in place to capture and effectively detect and/or investigate fraud or material litigation should it be required; and
- Seek confirmation annually and as necessary from internal and external auditors, attending ~~Councillors~~Elected Members, and Management, regarding the completeness, quality and appropriateness of financial and operational information that is provided to the Council.

~~1.19~~1.18 Risk management

- Review and consider Management's risk management framework in line with Council's risk appetite, which includes policies and procedures to effectively identify, treat and monitor significant risks, and regular reporting to the Council;
- Assist the Council to determine its appetite for risk;
- Review the principal risks that are determined by Council and Management, and consider whether appropriate action is being taken by Management to treat Council's significant risks;
- Assess the effectiveness of, and monitor compliance with, the risk management framework; and
- Consider any emerging risks trends and report these to Council where appropriate.
- To examine and consider the transfer of risk through an annual review of Council's insurances.

~~1.20~~1.19 Internal audit

- Review and approve the annual internal audit plan, which is to be based on the Council's risk framework;
- Monitor performance against the annual audit plan at each regular quarterly meeting;
- Monitor all internal audit reports and the adequacy of Management's response to internal audit recommendations;
- Review six monthly fraud reporting and ensure fraud issues are disclosed to the external auditor;
- Provide a functional reporting line for the internal audit and ensure objectivity and transparency of the internal audit;
- Oversee and monitor the performance and independence of both the internal auditors and co-sourced auditors who may be appointed from time to time;
- Review the range of services provided by the co-sourced partner and make recommendations to Council regarding the conduct of the internal audit function; and
- Monitor compliance with Council's delegation policies.

~~1.21~~1.20 External reporting and accountability

- Consider the appropriateness of the Council's existing accounting policies and practices and approve any changes as deemed appropriate;
- Contribute to improve the quality, credibility and objectivity of the accounting processes, including financial reporting;
- Consider and review the draft annual financial statements and any other financial reports that are to be publicly released and make recommendations to Management on any matters that arise from those statements or reports;
- Consider the underlying quality of the external financial reporting, including:
  - changes in accounting policy and practice;
  - any significant accounting estimates and judgements, accounting implications of new and significant transactions, management practices;
  - and any significant disagreements between Management and the external auditors; and

- the propriety of any related party transactions and compliance with applicable Australian and international accounting standards and legislative requirements.

- Consider the disclosure of contingent liabilities and contingent assets as well as the clarity of disclosures generally;
- Consider whether the external reporting is consistent with Committee members' information and knowledge, and whether it is adequate for stakeholder needs;
- Recommend to Council:
  - the adoption of the Financial Statements and Reports; and
  - the Statement of Service Performance; and
  - the signing of the Letter of Representation to the Auditors by the Mayor and the Chief Executive Officer.
- Enquire of external auditors any information that affects the quality and clarity of the Council's financial statements, and assess whether appropriate action has been taken by Management;
- Request visibility of appropriate management signoff on the financial reporting and on the adequacy of the systems of internal control; including:
  - certification from the Chief Executive Officer, and other staff that risk management and internal control systems are operating effectively.
- ~~Consider and review the Community Strategic Plan Term and Annual Plans before adoption by the Council;~~
- Apply similar levels of enquiry, consideration, review and management sign off as are required above for external financial reporting; and
- Review and consider the Summary Financial Statements for consistency with the Annual Report.

~~1.22~~1.21 External audit

- Review and monitor whether Management's approach to maintaining an effective internal control framework is sound and effective, and in particular:
  - Review whether Management has taken steps to embed a culture that is committed to probity and ethical behaviour;
  - Review whether Management has in place relevant policies and procedures and how such policies and procedures are reviewed and monitored; and
  - Review whether there are appropriate systems processes and controls in place to prevent, detect and effectively investigate fraud.
- Annually review the independence of the audit engagement with the external auditor appointed by the Office of the Auditor General;
- Annually review the term of the audit engagement with the external auditor appointed by the Office of the Auditor General, including the adequacy of the nature and scope of the audit, and the timetable and fees;
- Review all external audit reporting, discuss with the auditors and review action to be taken by Management on significant issues and recommendations and report such actions to Council as appropriate;
- The external audit reporting should describe:
  - Council's internal control procedures relating to external financial reporting, findings from the most recent external audit and any steps taken to deal with such findings;

- All relationships between the Council and the external auditor;
- Critical accounting policies used by Council; and
- Alternative treatments of financial information within Generally Accepted Accounting Practice that have been discussed with Management, the ramifications of these treatments and the treatment preferred by the external auditor.

- Ensure that the lead audit engagement and concurring audit directors are rotated in accordance with best practice and Australian Auditing Standards.

~~1.23~~1.22 Compliance with legislation, standards and best practice guidelines

- Review the effectiveness of the system for monitoring the Council's compliance with laws (including governance legislation, regulations and associated government policies), with Council's own standards~~, and Best Practice Guidelines~~.

7 Late and urgent Business

Note: In accordance with Clauses 3.13 and 3.14 of the City of Kwinana *Standing Orders Local Law 2019*, only items resolved by the Audit and Risk Committee to be Urgent Business will be considered.

COMMITTEE DECISION

###

MOVED CR **SECONDED CR**

That the Audit and Risk Committee deal with the ..... items of urgent business as presented in the Addendum to the Agenda.

8 Confidential items

8.1 Office of the Auditor General (OAG) – Cyber Security Performance Audit

This report is confidential in accordance with Section 5.23(2)(e) of the *Local Government Act 1995*, which permits the meeting to be closed to the public for business relating to the following:

(e) a matter that if disclosed, would reveal –
(iii) information about the business, professional, commercial or financial affairs of a person

8.2 Update on OneCouncil Implementation Project

This report is confidential in accordance with Section 5.23(2)(c) of the *Local Government Act 1995*, which permits the meeting to be closed to the public for business relating to the following:

(c) a contract entered into, or which may be entered into, by the local government and which relates to a matter to be discussed at the meeting; and

9 Close of meeting