City of Cockburn
Audit Risk and Compliance Committee
Minutes

For Thursday, 25 May 2023

These Minutes are subject to confirmation

Presiding Member's signature

_____

Date: 27 July 2023

The Council of the City of Cockburn

**Audit Risk and Compliance Committee Meeting
Thursday, 25 May 2023 at 6pm**

Table of Contents

The Council of the City of Cockburn

Audit Risk and Compliance Committee Meeting
Thursday, 25 May 2023 at 6pm

Agenda

Present

Members
Cr K Allen (Presiding Member)
Deputy Mayor Widenbar (Arrive 6.01pm) (eMeeting)
Cr T Dewan
Cr P Corke
Mr G Geen

Observers
Cr C Reeve-Fowkes
Cr M Separovich

In Attendance
Mr D Arndt	A/Chief Executive Officer
Ms E Milne	Executive Governance and Strategy
Mr A Lees	Chief of Operations
Mr D van Ooran	Chief of Community Services
Mr C Catherwood	A/Chief of Built and Natural Environment
Ms C Hanrahan	A/Executive People Experience and Transformation
Mr N Mauricio	A/Chief Financial Officer
Ms M Todd	Manager Legal and Compliance
Mr B Fellows	Head of Information and Technology
Mr M Lee	System Support Officer (IT Support)
Mr J Fiori	Risk and Governance Advisor
Mrs S D'Agnone	Council Minute Officer

1. Declaration of Meeting

The Presiding Member declared the meeting open at 6pm.

2. Appointment of Presiding Member

N/A

3.   Disclaimer

The Presiding Member read the disclaimer:

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.

8.01pm   Deputy Mayor Widenbar entered the meeting.

4.   Acknowledgement of Receipt of Written Declarations of Financial Interests and Conflict of Interest (by Presiding Member)

Nil

5.   Apologies & Leave of Absence

Ms V Green, Executive Corporate Affairs - Apology

6.   Public Question Time

Nil

7.   Confirmation of Minutes

7.1   (2023/MINUTE NO 0005) Minutes of the Audit Risk and Compliance Meeting - 16/03/2023

Committee Recommendation
MOVED Cr T Dewan SECONDED Cr P Corke

The Committee confirms the Minutes of the Audit Risk and Compliance Meeting held on Thursday, 16 March 2023 as a true and accurate record.

CARRIED 5/0

8.   Deputations

Nil

9.   Business Left Over from Previous Meeting (if adjourned)

Nil

10.   Declaration by Members who have Not Given Due Consideration to Matters Contained in the Business Paper Presented before the Meeting

Nil

En Bloc Resolution

6.03pm   The following items were carried En bloc by simple majority:

11.1.1
11.2.1
11.3.1
11.4.3
11.5.1

11   Reports - CEO (and Delegates)

11.1 Built and Natural Environment

11.1.1 **(2023/MINUTE NO 0006)** Submission to the Office of the Auditor General – Performance Audit: Regulation of Air-handling and Water Systems

Responsible Executive	A/Chief of Built and Natural Environment
Author	A/Manager Public Health and Building Services
Attachments	1. OAG Performance Audit Report-20 21 April 2023 Regulation-of-Air-handling-and-Water-Systems ⇓

Officer Recommendation/Committee Recommendation
MOVED Cr T Dewan SECONDED Cr P Corke

That Council:

(1)   RECEIVES the attached Office of the Auditor General Regulation of Air-handling and Water Systems Performance Audit dated 21 April 2023 which seeks to minimise the risk of Legionella bacteria (in air-handling and water systems) which can result in a serious lung infection known as Legionnaire's Disease;

(2)   RECEIVES the report has been prepared by the Office of the Auditor General Western Australia for submission to Parliament under the provisions of the *Auditor General Act 2006*;

(3)   RECEIVES the purpose of the performance audit is to provide Parliament and the people of WA with opportunities for improved performance regarding the risk of Legionella bacteria; and

(4)   SUPPORTS the Office of the Auditor General recommendations.

CARRIED 5/0

Background

On 21 April 2023 the Office of the Auditor General (OAG) published Report 20: 2022-23 'Performance Audit Regulation of Air-handling and Water Systems'.

The Auditor General advises the performance audit has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006.*

Section 25 of the *Auditor General Act 2006* specifies;

1. *The Auditor General may prepare and sign a report on an examination or investigation carried out under section 18 and may submit the report to —*

   (a) both Houses of Parliament; or
   (b) the Public Accounts Committee and the Estimates and Financial Operations Committee

---

2. *Before signing a report proposed to be submitted under subsection (1), the Auditor General must —*

    (a) *give a summary of findings to the Treasurer, agency or audited local subsidiary, as the case may be, and any other person who, in the Auditor General's opinion, has a special interest in the report; and*

    (b) *by written notice, invite the Treasurer, the accountable authority of the agency, the audited local subsidiary or that other person, as the case may be, to make submissions or comments on the content of the summary of findings before a specified day, being not more than 14 days after the summary of findings is given to the Treasurer, agency, audited local subsidiary or person.*

This report provides a summary of the audit with a recommended submission to the OAG under section 25(2) of the *Auditor General Act 2006*.

Submission

N/A

Report

Purpose of the OAG Audit

In our community the growth of Legionella bacteria in air-handling and water systems can, in rare instances, result in a serious lung infection known as Legionnaire's disease.

An outbreak in Melbourne in 2020 resulted in 125 people hospitalised and four dead.

Fortunately, in Western Australia we have not experienced an outbreak. However, this doesn't mean it can't or won't occur.

The risk of an outbreak may increase as our infrastructure and population ages, the climate warms, and new uses for water in our built environment emerge.

The OAG audit examined three State entities, and three local governments: City of Joondalup, City of Melville and City of Perth, as they are enforcement agencies under the *Health (Air-handling and Water Systems) Regulations 1994* (the Regulations).

Significant matters identified by the OAG

The OAG audit report has identified the matters summarised below:

- The existing regulatory framework requires improvement. Current limitations to the Regulations reduce their effectiveness in minimising public health risk.
- There is inconsistency in how owners maintain and test their air-handling and water systems.
- Improved education and guidance for owners of air-handling and water systems is needed, ahead of updated legislation.

Implications for local government

At present the Department of Health conducts limited education or awareness activities relevant to air-handling and water systems as part of its oversight role.

While the local government sector and the industry have been advised of the likely framework for the new regulations, there is limited advice on how the public health risk should be minimised in the interim.

The Department of Health has commenced preparations for the introduction of new regulations under the *Public Health Act 2016*.

The City understands that planning documents for these regulations propose engagement with Local Government and industry through training presentations, letters, updated web content and guidelines.

The OAG report recommends that the Department of Health provides updated guidance to owners of systems high-risk settings, to assist the industry to achieve best practice.

Table 1: The City's draft submission to the OAG in relation to the OAG Performance Audit dated 21 April 2023 (Regulation of Air-handling and Water Systems):

No.	OAG recommendation	City Response
1.	The Department of Health, in consultation with local government entities should: (a) Review current guidance to industry and local government entities in preparation for the adoption of the proposed new regulatory framework (b) Develop and implement an education program to support and encourage system owners to achieve more consistent risk-based practice. (c) Establish and maintain a central register of air-handling and water systems within WA (d) Consider splitting the implementation of the environmental health regulation package under the *Public Health Act 2016* to focus on areas of highest priority, including the air-handling and water systems regulations.	The City of Cockburn supports this recommendation. The Built and Natural Environment division will continue to work with the Department of Health with the implementation of all necessary measures to adequately address and communicate the public health risk of air-handling and water to affected property owners. The Department of Health has indicated July 2024 as an implementation timeframe for these requirements.
2.	Local government entities, in consultation with Department of Health should: (a) develop ways to gather the information on air-handling and water systems in their areas that will support a central register (b) consider introducing a risk-based monitoring/compliance process for air-handling and water systems within their jurisdiction.	The City of Cockburn supports this recommendation. The Built and Natural Environment division will continue to maintain a register of the air-handling and water systems within the City and undertake modifications as necessary to meet the requirements of new regulations, within the indicated timeframe of December 2024.

| 3. | State and local government entities who own air-handling and water systems should:

(a) develop risk management plans
(b) ensure that systems are operated and maintained in accordance with Australian/New Zealand Standard 3666 *Air-handling and water systems of buildings–Microbial control.* | The City of Cockburn supports this recommendation.

The Built and Natural Environment division will continue to liaise with the Department of Health as it progresses development of a risk management and assessment framework for Legionella control. The Department of Health has indicated that this will be implemented by July 2024.

The Built and Natural Environment division will engage with local businesses to ensure that they are aware of their obligations to comply with Australian/New Zealand Standard 3666 *Air-handling and water systems of buildings–Microbial control.*

The City's Operations Division will continue to ensure that air-handling and water systems owned by the City are maintained in accordance with AS/NZS 3666. This may include replacement of older air-handling systems overtime. |

Conclusion

It is recommended the Committee notes the OAG'S performance audit and provides support of the above three recommendations.

Strategic Plans/Policy Implications

Listening & Leading
A community focused, sustainable, accountable and progressive organisation.
• Best practice Governance, partnerships and value for money.

Budget/Financial Implications

N/A

Legal Implications

Sections 7.1, 7.12A(3) and 7.12AJ of the *Local Government Act 1995* refer; and *Public Health Act 2016.*Community

Consultation

The OAG is currently consulting the community by way of the attached performance audit. Section 25 (2)(b) of the *Auditor General Act 2006* specifies the Auditor General must invite the public to make a submission or comments of the summary of findings before a specified day being not more than 14 days after the summary of findings.

Risk Management Implications

OAG performance audits constitute the fourth line of defence in the OAG's 'Four Lines of Defence Assurance Model' which the City has adapted in the *City of Cockburn Enterprise Risk Management Framework*.

The OAG has identified risks in its performance audit report and, as appropriate, the City will implement adequate appropriate control measures, where applicable.

Not following the OAG's audit recommendations would constitute a Substantial compliance risk.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

Office of the Auditor General
Serving the Public Interest

Report 20: 2022-23 | 21 April 2023
PERFORMANCE AUDIT

Regulation of Air-handling and Water Systems

Office of the Auditor General
Western Australia

*The Office of the Auditor General acknowledges the traditional custodians throughout
Western Australia and their continuing connection to the land, waters and community. We
pay our respects to all members of the Aboriginal communities and their cultures, and to
Elders both past and present.*

Image credit: Pedal to the Stock/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Regulation of Air-handling and Water Systems

Report 20: 2022-23
21 April 2023

This page is intentionally left blank

THE PRESIDENT   **THE SPEAKER**
LEGISLATIVE COUNCIL   **LEGISLATIVE ASSEMBLY**

REGULATION OF AIR-HANDLING AND WATER SYSTEMS

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

Performance audits are an integral part of my Office's overall program of audit and assurance for Parliament. They seek to provide Parliament and the people of WA with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

This audit assessed if the Department of Health and three local government entities regulate air-handling and water systems to minimise the risk of Legionella.

I wish to acknowledge the entities' staff for their cooperation with this audit.

Labuschagne

SANDRA LABUSCHAGNE
ACTING AUDITOR GENERAL
21 April 2023

Contents

Auditor General's overview

In our community the growth of Legionella bacteria in air-handling and water systems can, in rare instances, result in a serious lung infection known as Legionnaires' disease.

In Australia's largest outbreak of Legionnaires' disease at the Melbourne Aquarium in 2000, 125 people were hospitalised and four died. In the investigation that followed, Legionella was found in the Aquarium's cooling towers.

Thankfully WA has not experienced an outbreak of Legionnaires' disease, however this doesn't mean that it can't or won't occur. While individual cases remain rare, the risk of an outbreak may increase as our infrastructure and population ages, the climate warms and new uses for water in our built environment emerge.

As members of the public we do not often see or have access to air-handling and water systems. In fact, many of us would be unaware of their existence. Yet we are entitled to expect that they are effectively managed to minimise public health risks.

Our audit found inconsistencies in how owners maintain and test their systems. It also found that the existing regulatory framework requires improvement. The Department of Health has recognised this and is developing new regulations for air-handling and water systems. However, legislative change can be a long process and Legionella risks remain in the interim. Rather than await new legislation, I encourage all State and local government entities that own these systems to maintain and test in accordance with standards.

The Department of Health and the local government sector should also work together to support property owners through education and awareness, particularly for vulnerable and high-risk settings such as hospitals and aged care facilities.

Executive summary

Introduction

This audit assessed if the Department of Health (Department) and three local government entities (LG entities) effectively regulate air-handling and water systems to minimise the risk of Legionella. To consider how well this public health risk is managed we also included a sample of State government entities who operate these systems.

Background

Air-handling and water systems circulate water through built environments. Common examples include:

- cooling towers and evaporative air conditioners – devices commonly used for air cooling in hotels, hospitals, shopping centres, office towers and universities

- warm water systems – plumbing systems that distribute water at warm temperatures (approximately 40°C) to reduce the risk of scalding, often found in hospitals and aged care settings.

Wet surfaces within these systems can support the growth of viruses, fungi and bacteria. The most concerning risk is the growth of Legionella pneumpohila (Legionella) bacteria. These bacteria naturally occur in the environment but can proliferate in poorly managed systems. If water droplets containing these bacteria are inhaled, it can result in Legionnaires' disease (Legionellosis), see Figure 1.

Legionnaires' disease is a rare but potentially life-threatening lung infection. Symptoms include fever, muscle and joint pain, headaches, dry cough and shortness of breath. Older adults, current or former smokers and people with weakened immune systems are at an increased risk of infection.
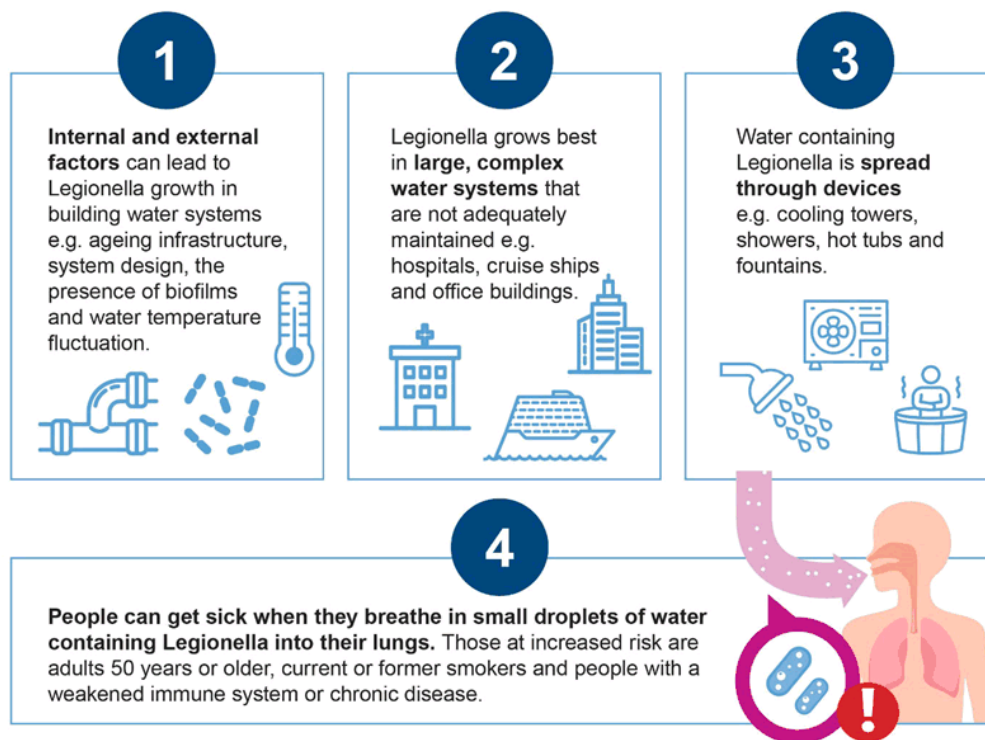
Source: OAG based on US Centers for Disease Control and Prevention information

Figure 1: Common sources and transmission of Legionella bacteria from water systems

The Health (Air-handling and Water Systems) Regulations 1994 (the Regulations) detail the requirements for the design, installation, maintenance and operation of air-handling and water systems.

The Regulations are based on the Australian/New Zealand Standard 3666 titled *Air-handling and water systems of buildings – Microbial control* (the Standard). The Standard details minimum requirements for installing, operating and maintaining air-handling and water systems, with the aim of minimising health risks from viruses, fungi and bacteria.

We examined a selection of State and LG entities that have various responsibilities under the current Regulations (Figure 2):

- Department – lead regulator, as well as system manager for Health Service Providers (HSPs). HSPs are responsible for the delivery of health services within their local communities and manage infrastructure including air-handling and water systems in WA public hospitals.

- Three LG entities – the Cities of Joondalup, Melville and Perth were selected as they are enforcement agencies under the Regulations. All three LG entities also have buildings with air-handling and water systems within their boundaries and two are owners of cooling towers. The Department estimates the majority of LG entities in Western Australia (WA) have cooling towers or warm water systems within their boundaries.

- Three State entities that own and operate several different types of air-handling and water systems. Two HSPs, the North Metropolitan Health Service (NMHS) and WA Country Health Service (WACHS) were included as hospital settings are considered at

increased risk of Legionella due to their design and need to accommodate vulnerable populations. The other State entity selected was the Department of Local Government, Sport and Cultural Industries (DLGSC), who runs buildings open to the public, including museums, galleries and theatres.

Department of Health

Lead regulator and system manager for WA Health.

Local government

Regulatory agency for air-handling and water systems within jurisdiction. LG entities should approve applications for new or substantially modified systems and have the authority to close systems suspected of causing a serious risk to health.

Owners of air handling and water systems

Responsible for maintaining and sampling system in accordance with AS3666 e.g. hospitals, aged care homes, office buildings and large public buildings.

Source: OAG

Figure 2: Current regulatory framework for air-handling and water systems

When administering regulation, it is important that the health of the community and a reasonable expectation of compliance is considered. A risk-based approach, that considers the consequences of an actual or potential event and the likelihood of occurrence is vital.

Conclusion

The number of notified cases of Legionnaires' disease is relatively low in WA, and there has not been an outbreak as has occurred in other states. But exposure to Legionella from air-handling and water systems remains a public health risk with potentially serious consequences, particularly for vulnerable groups. The existing regulatory framework requires improvement to ensure it effectively minimises the risk. Gaps in the current arrangements result in limited monitoring and information so it is not clear if low case numbers are the result of good practice by system owners, environmental factors or both.

The Department completed a review of the current regulatory arrangements in 2021 and has recommended new legislation that would update the regulatory approach in WA and see the Department take on responsibility for high-risk settings and State-owned buildings. However, the legislation forms part of a broader reform program and may take some time to introduce and implement. The differences we observed in how owners monitor and maintain their systems demonstrate that better education and guidance from the Department's public health unit is needed ahead of updated legislation.

Findings

Case numbers are low and there have been no outbreaks identified in WA

Legionnaires' disease is an urgently notifiable disease and must be reported to the WA Chief Health Officer within 24 hours of confirmation. Historically WA has experienced low levels of the illness, with no outbreaks[1] identified since the introduction of the Regulations in 1994. Data provided by the Department indicates that a total 188 cases were reported over the last 10 years (2013-2022). In 2022, there were 24 cases, with a slight upwards trend noted in cases over the 10 years examined (Figure 3).
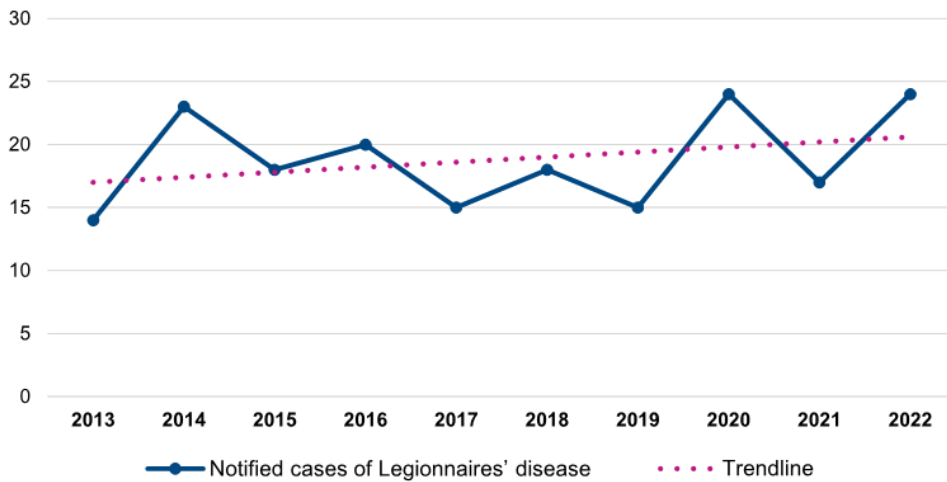
Source: OAG

Figure 3: Numbers of notified Legionnaires' disease cases in WA over a 10-year period

Of the 188 cases in the past 10 years:

- 132 were suspected as being acquired in the WA community

- 46 were suspected to be acquired interstate or overseas

- five were suspected as being acquired in a WA hospital

- five were of an unknown source.

As with many notifiable diseases, the true number of cases may be higher as under diagnosis and under reporting may be present.

While the overall community risk posed by Legionella appears to be low, hospital and aged care settings are of particular concern. These facilities frequently feature both warm water systems and cooling towers in an environment that caters to highly vulnerable people who have increased susceptibility and likelihood of severe consequences from Legionnaires' disease. Currently the Regulations do not provide specific guidance or particular focus on higher risk groups or settings.

---

[1] Two or more cases linked in time and place to a common source.

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Gaps in the current Regulations reduce their effectiveness in minimising the public health risk

Roles and responsibilities are fulfilled inconsistently by LG entities

Roles and responsibilities for regulators and owners are articulated under the Regulations and the Standard. However, the Department acknowledges the Regulations are poorly applied across LG entities and concedes authorised officers within LG entities may not have the specialised skills and knowledge required for air-handling and water systems. In the absence of guidance, LG entities are waiting for the new regulations to provide clarity on what they should be doing.

Currently the main activity of LG entities relevant to air-handling and water systems is case investigation. The Department completes an initial case investigation and then requests assistance from LG entities to contact and attend sites that have been visited by a Legionnaires' disease patient and have an air-handling or water system onsite. The relevant LG entity then collects water samples from systems identified and submits these samples to the State laboratory for Legionella testing.

We examined a summary of investigation data for 37 community acquired cases investigated by the Department over a three-year period from 2020 to 2023. A potential source was identified in 10 of the cases, meaning approximately 70% had no known source identified. While determining a source is not always possible, we noted several examples of incomplete case investigations, with the Department citing a lack of participation or response from the LG entity involved. None of the investigations involved the three LG entities included in this audit.

The Department and LG entities do not have accurate records on the number, type and location of air-handling and water systems

A key limitation of the current framework is the lack of accurate records detailing the type and location of air-handling and water systems. All three LG entities in our sample had registers for air-handling systems located within their boundaries but these were not complete or current. Having accurate and readily accessible system details is important for a timely and effective public health response to a Legionella outbreak.

Delays in identifying a contaminated system can mean that more individuals are exposed, particularly in busy public environments, as the system is not swiftly identified and decontaminated or shutdown. There is also a risk that Legionella can spread from a contaminated system to those within the surrounding area. Timely access to accurate details of systems within a nominated geographical area is therefore important.

Several attempts by LG entities to collate and maintain accurate records were evidenced, however activity has been sporadic and suffered from a lack of response from system owners. In 2017, the Department unsuccessfully attempted to determine the number of cooling towers and water systems within WA. It estimates there are approximately 3,000 sites fitted with a cooling tower and 400 vulnerable premises fitted with a warm water system, but the true numbers could be higher.

The Department has proposed a central register that it will collate and manage with input from LG entities who have systems within their boundaries. Details on the establishment and maintenance of the register are yet to be considered and its success will depend on timely submission of information. It is important that information on systems in higher risk settings (i.e. hospitals and aged care facilities) be prioritised for complete and accurate record keeping.

LG entities use the certified building licence process to assess and approve new or significantly modified systems

The Regulations require LG entities to provide written approval to a person who proposes to install or significantly modify an air-handling or water system. However, the three LG entities were unable to demonstrate a consistent process for assessing or approving the installation of new or significantly modified systems that complied with the Regulations.

The Department has identified a lack of a prescribed format for submission and approval as one of the barriers to LG entities meeting this requirement. There may also be a lack of awareness about the requirement by industry and potentially limited technical expertise within LG entities. For example, the three LG entities did not inform potential owners/builders of their obligation to apply to install a new or significantly modified system via their website.

The three LG entities rely on the certified building licence process to confirm that a commercial development complies with the National Construction Code and it's adopted standards.

The certified building licence process allows for assessment of system design and installation requirements by those with specialised technical expertise and is the Department's proposed arrangement for new regulations.

The limited monitoring and information required under current regulations reduces assurance on whether systems are being effectively maintained

The existing regulatory framework does not require compliance monitoring activities by either the Department or LG entities. This means that information on how well owners are managing their systems is limited, and reduces the level of assurance on whether systems are being effectively maintained.

At present, the regulatory framework relies on self-regulation by owners. While self-regulation is common and appropriate in many sectors, the Department has assessed (including through public consultation) that as serious illness or death could eventuate from mismanagement of air-handling and water systems, a regulated approach is required.

The current Regulations enable but do not oblige LG entities to conduct inspections of air-handling and water systems within their jurisdiction. We found that two of the three LG entities do not conduct any or only limited monitoring activities. The third LG entity did conduct annual inspections of five cooling towers known to be in their jurisdiction, using an inspection template based on the Standard. Limited monitoring means the detection of non-compliance and use of enforcement powers are also limited. Under the current arrangements the first indicator of an issue is most likely to be the notification and subsequent investigation of a Legionnaires' disease case. More consistent risk-based compliance monitoring would move from a reactive to a more preventative approach.

The *Health (Miscellaneous Provisions) Act 1911* does not bind the Crown, meaning State government entities are not covered by the requirements of the current Regulations. New regulations under the *Public Health Act 2016* will require monitoring and compliance of all owners, including State government entities. However, it is reasonable to expect that managing the risk of Legionella in vulnerable facilities, particularly those owned by the State, should be prioritised while the new regulations are in progress.

There is inconsistency in how owners maintain and test their air-handling and water systems

Owners respond differently to detections that should produce a uniform response

The Standard sets out the minimum requirements for regular routine maintenance. Where these requirements are not practical (i.e. where systems need to be shutdown), the Standard provides an alternative approach based on regular testing and specifies the action to be taken in response to a detection of Legionella. Table 1 shows the control strategies as determined by the test result and the number of Legionella bacteria identified.

Legionella test result (cfu*/mL)		Required control strategy
	Not detected (<10)	• System under control • Maintain monitoring and treatment program
	Detected as <1,000	• Immediate decontamination (alternative or higher dose of biocide than usual) • Review control strategy • Re-test within 3-7 days of plant operation • Assess if further remedial action is necessary
	Detected as ≥ 1,000	• Immediate decontamination (chlorine-based biocide) • Review control strategy • Re-test within 3-7 days of plant operation • Assess if further remedial action is necessary

Source: OAG based on Department of Health information

colony forming units

Table 1: Control strategies for the presence of Legionella

We found the Standard was not consistently followed because different owners tested at different frequencies and took different actions in response to detections. Inconsistent application of the Standard does not align with best practice and reduces confidence that the risk from Legionella is effectively managed.

The State and LG entities we reviewed were aware of the number of air-handling and waters systems they owned and were responsible to maintain. They all had asset registers that included these systems. Our sampled entities owned 87 air-handling and water systems, comprising 20 cooling towers and 67 warm water systems.

Two LG entities, DLGSC and the two HSPs were able to provide documented evidence for Legionella testing of the systems they owned. In the two HSPs who manage systems in high-risk settings, we found the frequency of testing varied depending on the hospital site. For example, the regularity of cooling tower testing varied from once a month to no testing within a two-year period.

Regular testing is important because it provides assurance and mitigates the risk of an outbreak. Results in the two HSPs showed:

- detection of Legionella was more common in warm water systems than cooling towers

- since July 2020 one HSP performed a total of 3,309 Legionella samples. An average of 4.6% of samples detected Legionella and required remedial flushing and/or thermal disinfection. Overall this percentage has declined over time. Where legionella was detected, the Department advised that 50% of those detections were borderline results (i.e. 10 CFU/ml)

- a total of four cooling towers samples showed a Legionella detection in the two-year period we reviewed

- the other HSP provided results for 803 water samples in 2022. These results showed Legionella was detected in 6.5% of the samples. While there is no evidence of any hospital acquired cases of Legionnaires' disease within this HSP, we found inconsistencies in record keeping including a lack of consistent remedial action. This indicates a need for greater management oversight across various sites.

Case study 1: Example of HSP activity in Legionella management and prevention

One HSP has invested significantly in the management of its on-site water systems. Initiatives include:

- the adoption of an overarching Water Quality Management Policy and Framework that defines the requirements and outcomes for effective onsite water management

- the development of site-specific Facility Water Safety Plans that detail the individual characteristics of systems and risks that are present at each site

- a risk-based monitoring and validation program

- the implementation of management software to record and document water monitoring activities.

A review of these initiatives undertaken by the Department indicated some area for improvement but in general found that the Water Quality Management System provided a reasonable risk-based framework for identifying and managing water quality risks.

The Department is developing a universal water risk management framework and assessment tool for HSPs to encourage consistency and reduce risk

In December 2021, the Department initiated a review of processes and procedures by HSPs to control Legionella. The review indicated there were varying strategies between HSPs to minimise and control Legionella in their water-based systems which could reduce the level of assurance and increase risk.

Following the completion of the review, work has started in the Department to develop a universal water risk management framework for Legionella control and a risk assessment tool for HSPs. The purpose of the risk assessment tool is to identify potential gaps and improvement opportunities within State owned health facilities. Six pilot hospital sites (three metropolitan and three regional) have been selected to trial the risk assessment tool.

The pilot program is scheduled for completion by July 2023 with the results to be presented to WA Health's Executive Committee. The implementation timeframe for the framework is yet to be established but the Department anticipates this work will benefit vulnerable settings, LG entities and the industry more broadly to standardise better practice, ensure consistency and reduce risk.

Aged care facilities have both warm water systems and vulnerable people, but little is known about how well their systems are managed

Aged care facilities are a high risk due to a combination of warm water systems and vulnerable people but are mostly privately owned and operated with little known about how well systems are managed. The LG entities we spoke to have limited awareness of warm water systems within their jurisdiction. Larger aged care facilities may also feature the use of cooling towers.

The Department liaised directly with the Commonwealth Aged Care Quality and Safety Commission regarding its proposed new regulatory requirements. The Commission informed the Department that the Aged Care Quality Standards do not include specific requirements relating to air-handling and water systems. Accordingly, the Department intends to ensure that aged care facilities are captured by the new regulations but there is nothing to address the risk in the interim.

New regulations are likely to take some time, better guidance and education would help reduce risk in the interim

The Department has identified the need to update the regulatory framework

In 2017 the Department started a review of the current Regulations. The review encompassed all subsidiary legislation under the *Health (Miscellaneous Provisions) Act 1911* and covered a wide range of public health risks such asbestos, drinking water and public events. For air-handling and water systems the review included two consultations to seek the opinions and potential impacts of any proposed changes on industry, LG entities and other interested parties.

The review found that the Regulations have several limitations and are inconsistently administered by LG entities. Specifically, there is no requirement for air-handling and water system registration, no notification requirement when elevated levels of Legionella are detected and no requirements for maintenance and testing to be reviewed or checked. Further, in the event of non-compliance with the Regulations, enforcement options are limited and the maximum penalty is $1,000.

A key purpose of the review was to determine the most effective options for managing the public health risk of air-handling and water systems into the future. Four options were considered:

A.   Deregulate to enable self-regulation and provide an industry guideline or code of practice.

B.   Develop equivalent regulations under the *Public Health Act 2016* and retain the status quo.

C.   Develop new regulations to manage the public health risk, with building requirements addressed by the Building Code of Australia.

D.   Manage the public health risk under occupational safety and health legislation.

The Department and respondents who participated in the consultation strongly supported option C. This position was informed by a public health risk assessment undertaken as part of the consultation. The assessment classified the public health risk of death from Legionella as high and the risk of illness as medium. These classifications indicate that control measures are necessary to mitigate and manage the public health risk to the community.

The Department has designed new regulations, but they will take time to enact and implement

Following the outcome of the review the Minister for Health approved the drafting of new regulations. The Department has completed policy instructions to inform the drafting process. The proposed regulatory framework for air-handling and water systems is detailed in Figure 4.

Under the new regulations the Department intends to take responsibility for regulating hospitals (both public and private), aged care facilities and all State-owned buildings. LG entities will be responsible for privately owned cooling towers within their boundaries. Further changes include requiring or adopting:

- the responsible person where a cooling tower or warm water system is located, to register each system with the appropriate enforcement agency. A prescribed form for registration and certificates of approval will be introduced

- the installer of systems to certify that the system has been designed and installed in accordance with the applicable requirements of the Building Code of Australia, as a requirement of system registration

- mandatory risk management plans for all systems

- minimum maintenance and performance-based testing requirements for systems

- mandatory reporting requirements for specified Legionella detection limits in systems.
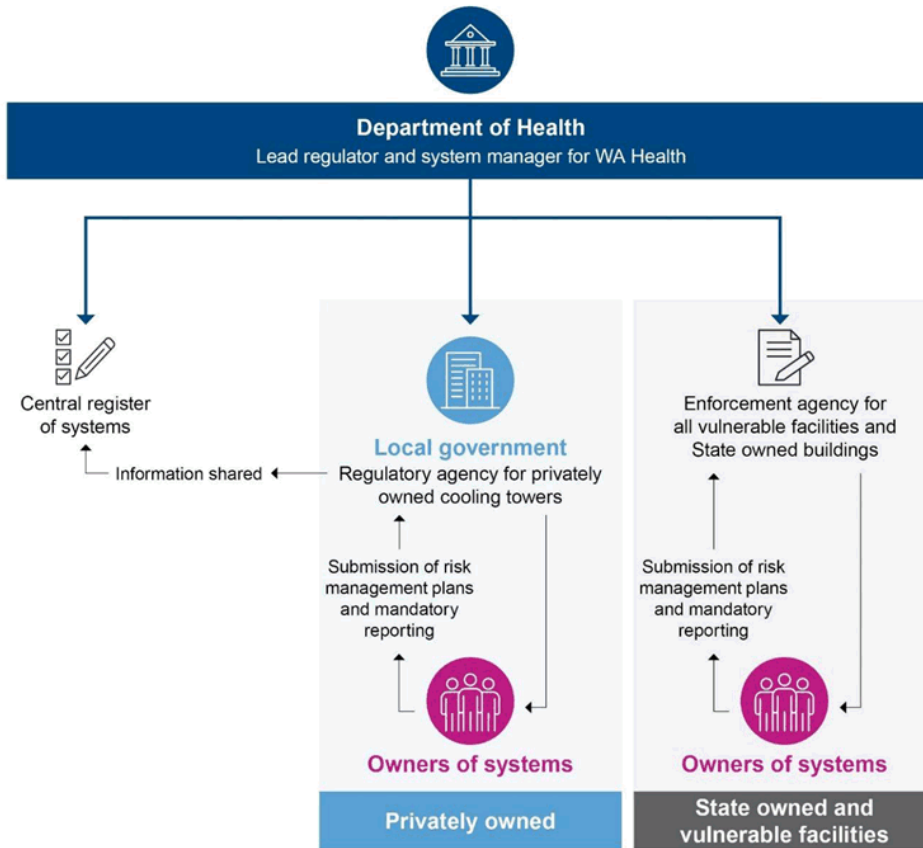
Source: OAG

Figure 4: Proposed regulatory framework for air-handling and water systems

Regulation of Air-handling and Water Systems | 15

The proposed changes align with arrangements in other jurisdictions such as Victoria. While an official timeframe has not been established, the Department had indicated that the proposed package of new environmental health regulations under the *Public Health Act 2016* may not be in place for at least two years. It has now advised that the individual regulations may be introduced separately based on priorities and risk.

Improved education and guidance is needed ahead of updated legislation

Currently the Department is conducting limited education or awareness activities relevant to air-handling and water systems as part of its oversight role. While the local government sector and the industry have been advised of the likely framework for the new regulations there is limited advice on how the public health risk should be minimised in the interim. This leads to a current holding pattern that awaits the implementation of the new regulations.

The Department has commenced preparations for the introduction of the new regulations. We reviewed planning documents that proposed engagement with LG entities and industry through training presentations, letters, updated web content and guidelines. However, these activities have no timeframe assigned. In the meantime, the Department should provide updated guidance to owners of systems particularly in vulnerable or high-risk settings to help ensure they adopt better practice.

Recommendations

1. The Department of Health, in consultation with local government entities should:

   a. review current guidance to industry and local government entities in preparation for the adoption of the proposed new regulatory framework

   b. develop and implement an education program to support and encourage system owners to achieve more consistent risk-based practice

   c. establish and maintain a central register of air-handling and water systems within WA

   d. consider splitting the implementation of the environmental health regulation package under the *Public Health Act 2016* to focus on areas of highest priority, including the air-handling and water systems regulations.

Implementation timeframe: July 2024

Department of Health response:

Recommendation supported.

The Department will review all current regulatory guidance material on the website for our co-regulators and industry and develop any information required which reflects the requirements for compliance with the Australian Standards that are at the core of best practice management of air handling and warm water systems currently and central to the proposed regulations being developed under the *Public Health Act 2016*. This approach will inform system owners and operators and other regulatory entities of what is proposed in the future and encourage transition to anticipated management practices that will provide more oversight.

The Department will develop guidance material and training to promote the proposed regulations and the expectations for future compliance to effect better risk-based management of systems.

The establishment of a central register was identified through consultation as a key requirement for the Department to undertake and manage to support implementation of new regulations. Considerations such as procurement of a suitable platform to host a register, how the information will be collected from third parties, how access to the registration information will be managed for the public and co-regulators and the cost for the register and staffing to maintain it, shall be factored into a forward work plan. In the meantime, the Department will inform co-regulators and industry of the intention to establish a register with the information that is likely to be required and the process to be adopted. In line with recommendations 1a and 1b, information relevant to these stakeholders about a proposed centralised register will be prepared in advance of any implementation.

DLGSC response:

The Department of Local Government, Sport and Cultural Industries is supportive of this recommendation.

2. Local government entities, in consultation with Department of Health should:

   a. develop ways to gather the information on air-handling and water systems in their areas that will support a central register

   b. consider introducing a risk-based monitoring/compliance process for air-handling and water systems within their jurisdiction.

Regulation of Air-handling and Water Systems | 17

Implementation timeframe: December 2024

City of Joondalup response:

Supported

City of Melville response:

Supported

City of Perth response:

Supported

3. State and local government entities who own air-handling and water systems should:

    a. develop risk management plans

    b. ensure that systems are operated and maintained in accordance with Australian/New Zealand Standard 3666, Air-*handling and water systems of buildings – Microbial control.*

Implementation timeframe: July 2024

Department of Health response:

Recommendation supported. Work by the Department is already underway.

DLGSC response:

The Department of Local Government, Sport and Cultural Industries is supportive of this recommendation. The development by the Department of Health of a universal water risk management framework for Legionella control and a risk assessment tool that can be adopted by all State and Local Government entities would support implementation of this recommendation.

City of Joondalup response:

Supported

City of Perth response:

Supported

Response from the Department of Health

The Department has proactively commenced preparations for the implementation of a stronger regulatory process for air-handling and warm water systems. The Department will support stakeholders through the transition to effect better risk-based management of systems. Health System Providers are reviewing legislative requirements and developing quality assurance mechanisms and educational tools.

Response from the City of Joondalup

The City of Joondalup appreciates the opportunity to participate in the Office of the Auditor General performance audit on the regulation of air-handling and water systems. The City acknowledges the public health risks posed by air-handling and water systems and supports the recommendations provided.

The City recognises its obligations as an owner of air-handling and water systems, to ensure that appropriate operational and maintenance activities continue to be performed to manage any risk to public health.

The City also understands the importance of its role in promoting public health and that local governments are typically well placed to engage with businesses to provide advice on legislative obligations and monitor for compliance.

The City looks forward to working with the Department of Health in the lead up to a new regulatory framework that will be introduced as part of phase 5 implementation of the *Public Health Act 2016* and is confident that new regulations and any associated guidance will provide improved and consistent management of air-handling and water systems.

The City acknowledges that a new regulatory framework is approximately two years away. The City is committed to implementing the recommendations to ensure that the current risks associated with air-handling and water systems are being addressed.

Response from the City of Melville

We thank the Office of the Auditor General for the opportunity to participate in the Performance Audit which provide a valuable contribution to identifying opportunities for improvement.

Response from the City of Perth

On balance, the City accepts and welcomes the audit findings. The City has a strong risk based community/environmental health programme. While oversight of air-handling and water systems attracts a lower risk profile than other enforcement responsibilities (e.g., food safety, aquatic facility safety, lodging house), opportunity for improvement is acknowledged. The City is committed to continuous improvement and looks forward to working with the Department of Health on this matter.

Response from the Department of Local Government, Sport and Cultural Industries

The Department of Local Government, Sport and Cultural Industries (DLGSC) accepts the findings of this audit. DLGSC is supportive of improved practices regarding the Regulation of Air-handling and Water Systems that take a risk-based approach and are in line with the Australian/New Zealand Standard *3666 Air-handling and water systems of buildings – Microbial control*. This includes the support of revised and/or new legislation to achieve this outcome.

Audit focus and scope

The objective of this audit was to assess if the Department of Health and local government entities effectively regulate air-handling and water systems to minimise the risk of Legionella.

We based our audit on the following criteria:

- Are sound arrangements in place for the management and oversight of the Legionella risks for air-handling and water systems?

- Do entities that regulate air-handling and water systems effectively administer requirements?

As part of this audit we:

- reviewed documentation related to the regulation of air-handling and water systems

- analysed available data from the Department of Health, North Metropolitan Health Service, WA Country Health Service, Department of Local Government, Sport and Cultural Industries and three local government entities (City of Joondalup, City of Melville and City of Perth)

- interviewed key staff at audited entities

- visited sites to view air-handling and water systems in operation.

Individual cases of Legionnaires' disease were not examined in relation to their potential sources, action/s taken or the investigation outcome.

A different sub-species of Legionella (Legionella longbeachae) can be found in soils and compost products and can also result in illness. This audit did not include Legionella longbeachae.

This was an independent performance audit, conducted under section 18 of the *Auditor General Act 2006*, in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other ethical requirements related to assurance engagements. Performance audits focus primarily on the effective management and operations of entity programs and activities. The approximate cost of undertaking the audit and reporting was $225,000.

Auditor General's 2022-23 reports

Number	Title	Date tabled
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation for Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

**Office of the Auditor General
Western Australia**

7ᵗʰ Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General
for Western Australia

11.2 Finance

11.2.1 **(2023/MINUTE NO 0007)** Cyber Risk Essential 8 Maturity Assessment

Responsible Executive	A/Chief Financial Officer
Author	Head of Information Technology
Attachments	1. LGIS - Essential 8 Assessment Report - Cockburn - Final ⇩
	2. City Information & Cyber Security Policy ⇩
	3. ISO 27001 Gap Assessment 2021 **(Confidential)**
	4. ISO 27001 Gap Assessment 2018 **(Confidential)**

Officer Recommendation/Committee Recommendation
MOVED Cr T Dewan SECONDED Cr P Corke

That Council:

(1)   RECEIVES the LGIS/Marsh ASD Essential 8 Controls Maturity assessment, as attached to the Agenda.

CARRIED 5/0

Background

The City's Insurance Provider, LGIS, commissioned a cyber security audit on a select group of local government entities. This audit informs the cyber security insurance premium paid by LG entities.

The cyber audit, carried out by Marsh Cyber Advisory, is based on the Australian Cyber Security Centre's (ACSC) Essential Eight (E8) - Essential Eight | Cyber.gov.au.

This is the City's first assessment against the E8.
The Essential Eight are practical guidelines, developed by the Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC), to mitigate cybersecurity incidents that include:

- The prevention of malware delivery and execution
- Limiting the extent of cybersecurity incidents
- Ensuring data recovery and system availability.

The E8 contains 8 cyber controls:

1.   Application Control (Whitelisting)
2.   Patch Applications
3.   Block Microsoft Office Macros
4.   User Application Hardening
5.   Restrict Administrative Privileges
6.   Patch Operating Systems
7.   Implement Multi-Factor Authentication
8.   Perform Daily Backups

The ASD E8 measures against a maturity model for each control, with maturity scores ranging from zero (0) (weakest) to three (3) highest. LGIS/Marsh minimum desired maturity level is two (2) for each E8 control.

The ACSC state "Maturity Level Three (3) will not stop adversaries that are willing and able to invest enough time, money and effort to compromise a target", and should consider further mitigation strategies beyond the E8.

Essential Eight Maturity Model | Cyber.gov.au

Submission

N/A

Report

Result of Assessment

The City scored an overall maturity level of 0.97 out of 3. The score reflects a poor maturity level across the ASD Essential 8 controls, indicating there is room for improving the City's overall cyber security mitigation strategy.

Recommendations have been provided as part of the assessment to enable the City to reach an overall maturity level score of 2.0, considered the baseline for a local government entity like Cockburn.

It is worth noting that work has already progressed since the assessment that will lead to an improved maturity score. An example is the recently implemented Security Information and Event Management (SIEM) technology that supports threat detection, compliance, and security incident management.

This was the number one priority for the City's recently commenced Cyber Security Officer and it will deliver greater intelligence for protecting against multiple cyber threats.

LGIS are in the last stages of finalising a benchmarking report for all the local governments that participated in the assessment. However, LGIS has indicated that a number of the City's scores of the LGIS Essential Eight (E8) areas are above average, while the rest are tracking closer to the average (showing a low maturity profile across the sector).

The pilot was undertaken by LGIS to assess the maturity and profile of the sector.

Ultimately, LGIS aim for an improved control environment across the sector to drive:

- Better availability of insurance coverage - maintaining cover and differentiating Local Government risk from the wider public sector (locally and internationally).
- Containing rising costs – cyber risk pricing is increasing and the (local government) portfolio effect will play a role in reducing the impact on pricing.

The LGIS/Marsh report also highlighted the following good practices at the City:

- Multi-Factor Authentication (MFA) very diligently implemented across organisation
- Privileged Access Management (PAM) diligently implemented and used within IT
- Documented backup processes with regular full backups
- Well-defined Windows patch management process
- Application Whitelisting diligently implemented

The City's Executive endorsed the first Information and Cyber Security Administration Policy in 2019 (attached). This policy aligns the City's Information Security Management Framework (ISMF) to the international standard of ISO 27001.

The ISO 27001 standard is a fully comprehensive list of controls, policies, risk management, procedures and technical and management controls designed to wholistically improve cyber security posture.

The ASD Essential Eight (E8) assessment is based on a set of tactical mitigation principles designed to protect Windows-based systems.

These mitigation strategies created by the Australian Cyber Security Centre that, when fully implemented provide protection from common cyber threats.

These principles have been defined at the federal level and are not specifically designed to protect cloud or non-Windows based systems which the City also uses.

Previous cyber audits at the City carried out by the Office of the Auditor General (OAG) were unofficially based on ISO 27002, which are not directly aligned to the Federal ASD E8. However, the WA State Government is following the ASD E8 protocol.

The City has also previously commissioned multiple ISO 27001 gap assessments (attached), with the most recent being December 2021.

Below is a summary of results from the most recent ISO 27001 gap assessment.

Domain	Current Status *
A.5 Policies	75%
A.6 Organisation	43%
A.7 HR security	83%
A.8 Asset management	25%
A.9 Access control	50%
A.10 Cryptography	25%
A.11 Physical security	80%
A.12 Operations security	64%
A.13 Communications	29%
A.14 System acq. dev. and maint.	54%
A.15 Supplier relationships	60%
A.16 Incident management	43%
A.17 Business continuity	38%
A.18 Compliance	25%

The City also commissioned an earlier ISO 27001 gap assessment in 2018. This highlights the significant process the City has made in aligning to ISO 27001 and improving cyber security.

Standard	Section	Status
A.5	Information Security Policies	13%
A.6	Organisation of information security	1%
A.7	Human resources security	21%
A.8	Asset management	13%
A.9	Access control	14%
A.10	Cryptography	18%
A.11	Physical and environmental security	43%
A.12	Operations security	32%
A.13	Communications security	0%
A.14	System acquisition, development and maintenance	1%
A.15	Supplier relationships	20%
A.16	Information security incident management	0%
A.17	Information security aspects of business continuity management	0%
A.18	Compliance	7%

Overall Compliance	13%

Whilst there is overlap of security controls between ISO 27001, ISO 27002 and ASD E8, an assessment against each framework will yield differing results.

The ACSC note that Application Control (whitelisting) and Multi-Factor Authentication provide the strongest protection against cyber threats; the City's assessed maturity level was high against these controls.

The City will incorporate recommendations from the E8 assessment into its cyber roadmap and action plan currently being developed to address gaps identified through the ISO 27001 and ISO 27002 assessments, to meet policy objectives.

Marsh's findings are tabled below along with the City's response comment.

Control	Current State Summary of Findings	Assessed Maturity Level	City Comment
Restrict Administrator Privileges	1. Privileged accounts can still login to the unprivileged Operating environments 2. Privileged accounts (excluding privileged service accounts) are not prevented from accessing the internet, email and web services. 3. Windows Defender Credential Guard and Windows 4. Privileged access to systems and applications are not automatically disabled after 45 days of inactivity. 5. There is no unique Credentials for local administrator accounts and service accounts 6. Privileged access to systems and applications	0.60	1. Significant progress already made since the report was commissioned. 2. Review current controls for privileged accounts due June 2023 3. Continue work of distinguishing privileged and unprivileged accounts due August 2023

Control	Current State Summary of Findings	Assessed Maturity Level	City Comment
	are not automatically disabled after 12 months 7. Defender Remote Credential Guard are not enabled		
Regular Backups	1. There is no Business Continuity Plan (BCP) 2. Testing of backups are not conducted periodically 3. Restoration of backups not done 4. Unprivileged accounts are not prevented from modifying or deleting backups. 5. Users with Privileged accounts can still access backups	0.75	1. The City currently has a BCP in place, and updated this in March 2023 2. Scheduled testing of backups has since been introduced 3. Scheduled testing of restorations has since been introduced 4. Helpdesk staff currently have access to backups to perform data restores.
User Application Hardening	1. There is no documented hardening guidelines 2. Web browsers are not configured to block web advertisements 3. PowerShell is not configured to use	0	1. Hardening guidelines to be documented by June 2023 2. Web browsers to be configured to block web advertisements by June 2023 3. PowerShell to have secure controls applied by August 2023 4. Application

Control	Current State Summary of Findings	Assessed Maturity Level	City Comment
	Constrained Language Mode 4. PDF software is not blocked from creating child processes. 5. Blocked PowerShell script executions are logged 6. Microsoft Office is not blocked from creating executable content. 7. Microsoft Office is not blocked from injecting code into other processes. 8. Web browser, Microsoft Office and PDF software security settings cannot be changed by users		Whitelisting currently prevents all execution of process not whitelisted 5. PowerShell to have logging applied by August 2023 6. Application Whitelisting currently prevents all execution of process not whitelisted 7. Application Whitelisting currently prevents all execution of non-Office processes not whitelisted 8. Further user application hardening to be applied by December 2023
Patch Operating Systems	1. There is no vulnerability scanner to identify the missing patches or security vulnerabilities	0.6	1. The City has since implemented a vulnerability scanner to identify missing operating system (OS) patches
Patch Applications	1. Controls pertaining to patching of applications are not implemented	0	1. The City has since implemented a vulnerability scanner to identify missing applications patches. The same method to

Control	Current State Summary of Findings	Assessed Maturity Level	City Comment
	nor appropriate risk management practices are enabled in the environment 2. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are not applied within two weeks of release, or within 48 hours if an exploit exists. 3. A vulnerability scanner is not used at least daily to identify missing patches or updates for security 4. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are		apply OS patches will be applied to Applications by August 2023

Control	Current State Summary of Findings	Assessed Maturity Level	City Comment
	not applied within two weeks of release, or within 48 hours if an exploit exists, this is covered only as a part of Patch Cycle	0	
Configure Microsoft Office Macros	1. There are no Microsoft Macros settings enabled throughout the Organisation	0	1. Currently being investigated. The City's Enterprise resource planning (ERP) System uses macros extensively. The City will apply MS Office macro settings by September 2023 or raise this as a risk if required by the ERP.
Application Control	1. Application whitelisting control is not implemented throughout the organisation	2.8	1. The City scored above the minimum recommendation for this control. All laptops and desktops have whitelisting applied. Servers to have whitelisting applied by December 2023.
Multi Factor Authentication (MFA)	1. MFA used extensively throughout organisation	3.0	1. The City scored above the minimum recommendation for this control

Marsh also recommended some further next steps. These are not ASD E8 specific recommendations but will further improve the City's cyber security posture.

Marsh Further Recommendations	City of Cockburn Response
• Defining the risk profile for each control as a result of inadequacies in the current implementation of controls. This will help the council in drafting the right mitigation strategies and minimise the probability of Cyber Security breach / data breach that can be caused by internal or external threats	• The City will define a risk profile for each control as per the City's Risk Management Framework by June 2023.
• Define Data Classification policy document to identify the critical and non-critical data and strengthen the controls to protect the critical / confidential data handled by the council	• The City has already commenced defining a data classification policy based on WA state government data classification framework. This should be complete by January 2024.
• Create a roadmap, which is essentially a statement on the improvement areas and plan of action for implementation of the improvement areas. This is where the organisation will review the risk statements and categorise them into the relevant risk actions i.e., accept, mitigate, transfer or avoid	• A cyber roadmap is currently being developed by the City's recently appointed Cyber Security Officer. This will be complete by June 2023.
• Create the strategy for implementation of the improvements for which risk mitigation is selected as the action in the roadmap. The strategy takes into consideration the budget available for implementation of the controls and prioritises the actions accordingly over a time frame of 12-18 months	• The cyber roadmap will be incorporated into the City's Information and Technology Strategy.
• Development of cyber incident response plans and cybersecurity awareness training for employees of the council to minimise possibilities of unintentional internal attacks through negligence or unawareness	• The City has a Digital Forensics & Incident Response (DFIR) plan in place. This plan includes prepaid engagement with cyber security professional services should this response plan require invoking. This plan is currently being reviewed and will be complete by June 2023.

Strategic Plans/Policy Implications

<u>Listening & Leading</u>
A community focused, sustainable, accountable and progressive organisation.
• Employer of choice focusing on equity, innovation and technology.
• Best practice Governance, partnerships and value for money.

Budget/Financial Implications

Implementing cyber security protection controls involves acquiring hardware, and software, along with specialist skills necessary to operationalise and support these controls.

Given the enhanced focus on IT Controls and ongoing audits from LGIS, OAG, other stakeholders and an internal audit regime, additional funds will be requested through the budget process to ensure the City meets the required levels of cyber security protection.

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

The review of findings and recommendations contained in the ASD Essential 8 assessment (and other recent cyber security audits) help steer the future direction, development, and implementation of cyber controls at the City. This work aims to reduce cyber security risks and improve the City's cyber security posture in a constantly evolving cyber threat landscape.

Addressing the ASD E8 recommendations will reduce the City's risk from cyber-attack on the City's operational IT systems and potentially compromising the confidentiality, integrity, and availability of the City's data. This mitigates against potential financial loss to recover data, and any subsequent reputational loss.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

ASD ESSENTIAL 8 CONTROLS MATURITY ASSESSMENT

City of Cockburn
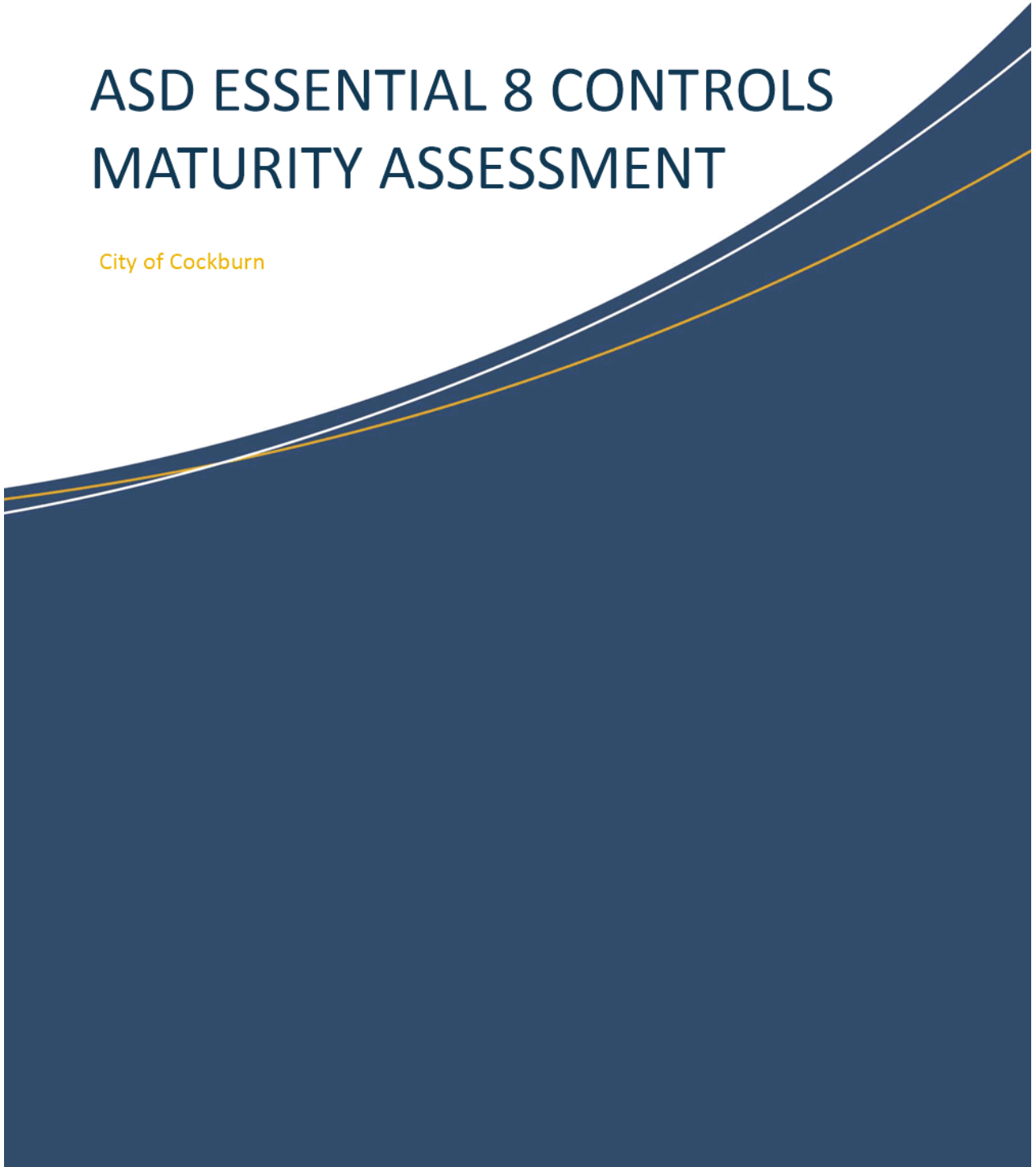
CONTENTS

ASD Essential 8 Controls
maturity assessment |
September 2022 | 2

EXECUTIVE SUMMARY

ASD Essential 8 is the most effective mitigation strategy developed by the Australian Cyber Security Centre (ACSC) to help all levels of government protect themselves against various cyber threats. Effective implementation of the controls listed under the mitigation strategy provides remediation for a major percentage of vulnerabilities that are typically identified for an organisation, and help reduce the probability for occurrence of cyber security incidents that occur through exploitation of untreated vulnerabilities.

Approach

The high level assessment is conducted by Marsh Advisory, on behalf of LGIS, to assess the risks associated with City of Cockburn's systems against ASD Essential 8 controls. This was an interactive session which was conducted for an overall 4 hours, split into two 2 hours sessions with "Brett Fellows – Head of Information & Technology", that was targeted at getting an understanding on whether and how the controls are implemented within the ecosystem. The assessment of ASD Essential 8 maturity is based on the survey responses captured during the interactive session and the supporting artefacts provided by the City of Cockburn. Post the interactive session, requirement for Artefacts were shared with the council for the controls discussed. Supplied artefacts were reviewed and captured for the overall maturity rating.

This is a first step towards getting a high-level view of compliance.

Result

The Council scored an overall maturity of 0.97 out of 3. The scores reflect a poor maturity level across the ASD Essential 8 controls. There is room for improving the overall mitigation strategy.

Recommendations are provided as part of the assessment to enable the **Council to elevate the overall maturity score to 2.0**, which is considered the baseline for non-corporate Commonwealth entities.

ASD Essential 8 Controls
maturity assessment |
September 2022 | 3

DEFINING THE ESSENTIAL 8 CONTROLS

The table below lists the Essential 8 controls and a description about what these controls are.

Sl No	Control	Description
1	Multi-factor Authentication (MFA)	An authentication method that requires the user to provide two or more verification factors to gain access to a resource
2	Restrict Administrator Privileges	Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive information. Restricting these accesses for relevant business use only is the mitigation strategy for over exposure of these privileges
3	Regular Backups	Information is the lifeline of an organisation and without the availability of critical business information, the organisation is unable to meet its mission critical requirements. Taking regular backups of critical information and systems ensures mitigation against loss of this data as a result of a cyber-incident such as ransomware, data breach, accidental or intentional data removal
4	User Application Hardening	Application hardening is a housekeeping of the application to ensure users have only those components or functions that they need access based on user roles and context (such as with application control). The hardening also calls for removal of sample files and default passwords, which can be leveraged by unauthenticated users to gain access to systems
5	Patch Operating Systems	Security patches are updated with latest fixes for newly discovered threats that can exploit vulnerabilities within the operating systems. Regular patching is a recommendation to ensure that fixes are updated into the operating systems The other requirement is to minimise the use of unsupported operating systems for which fixes are no longer created
6	Patch Applications	Just like operating systems, fixes are released by application vendors on a regular basis, but these need to be applied on the applications installed within the organisation for the control to be effective. As with operating systems, the out of support applications should be identified and their use within the organisation minimised
7	Microsoft Office Macro Settings	Microsoft Office applications can execute macros to automate routine tasks. However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion. Recommended mitigation is minimal use of macros in the environment and if macros are required for business purposes, use only those macros that are signed by trusted publishers
8	Application Control	Maintaining an inventory of applications that are required by the business to function and allow the use of only these applications within the organisation, whilst also disabling ability for end users to install applications or make configuration changes to bypass these controls

ASD Essential 8 Controls
maturity assessment |
September 2022 | 4

Each of the Essential 8 controls sit across 4 maturity levels. Each of the maturity levels and the significance of each level along with the risk to business as each of the maturity levels is documented below:

Maturity Level	Description and statement of risk
0	There are weaknesses in an organisation's overall cyber security posture. These weaknesses can be exploited to facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data
1	At this level, the adversaries seek to target common weaknesses in many targets rather than investing heavily in gaining access to specific target. They employ common social engineering techniques to trick users into weakening the security by launching malicious applications, for example via Microsoft Office macros. The other common targets are unpatched internet-facing systems, using stolen, reused, brute forced or guessed credentials to authenticate to an internet-facing service. If the account that an adversary compromises has special privileges they will seek to exploit it. Depending on their intent, adversaries may also destroy data (including backups).
2	At this level, the focus is on adversaries that have higher capability and who are willing to invest more time in a target and in the effectiveness of the tools. These adversaries will employ well-known techniques to bypass security controls implemented by the target to evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication. Generally, adversaries are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Adversaries will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications, for example via Microsoft Office macros. If the account that an adversary compromises has special privileges they will seek to exploit it, otherwise they will seek accounts with special privileges. Depending on their intent, adversaries may also destroy all data (including backups) accessible to an account with special privileges.
3	At this level, the focus is on highly skilled adversaries who are less reliant on public tools and techniques. These adversaries are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or inadequate logging and monitoring. Adversaries not only extend their initial access in a target, but also evades detection and solidify their presence. Adversaries are more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing policy and technical security controls implemented by their targets. This includes social engineering a user to not only open a document but also to unknowingly assist in bypassing security controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, adversaries will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, adversaries may also destroy all data (including backups).

As per the updated guidelines for the ACSC Essential 8 controls, it is recommended that all controls are at least at a baseline maturity level 2 and the overall maturity level is greater than 2.

THE ASSESSMENT

This section is segregated into listing down the good practices that the Council is following, result of the assessment with a summary of the controls maturity and control wise maturity rating, roadmap to improvement.

Good Practices

We analyzed the information provided and concluded that the City of Cockburn mostly aligns with the intent of the mitigation strategy based on their current state of controls listed as ASD Essential 8 and are following good practices in patching applications and taking daily backups of data that they categorize as important to their business

- Multi-Factor Authentication has been very diligently implemented within the Organisation.

- PAM Solution "Thycotic" is widely used within the IT team to manage the IT Privilege accounts

- A backup process is documented and regular full backups are taken to ensure business continuity during any disaster

- A patch management process has been defined and patches are updated automatically on all the workstations and servers via SCCM

- Application whitelisting is implemented across the Organisation

Result of Assessment

The table below shows the control wise maturity rating and the overall rating on the Essential 8 controls for the council.

Control	Score	Rating
Multi-factor Authentication (MFA)	3	🟩
Restrict Administrator Privileges	0.60	🟥
Regular Backups	0.75	🟥
User Application Hardening	0.0	🟥
Patch Operating Systems	0.60	🟥
Patch Applications	0.0	🟥
Microsoft Office Macro Settings	0.0	🟥
Application Control	2.8	🟩
Overall Rating (Average for the ratings for individual controls)	**0.97**	🟥

🟩 Strong (Greater than 2.0)

🟧 Moderate (Score between 1.0 to 2.0)

🟥 Poor (Lesser than 1.0)

Baseline Maturity Rating Vs Current Rating
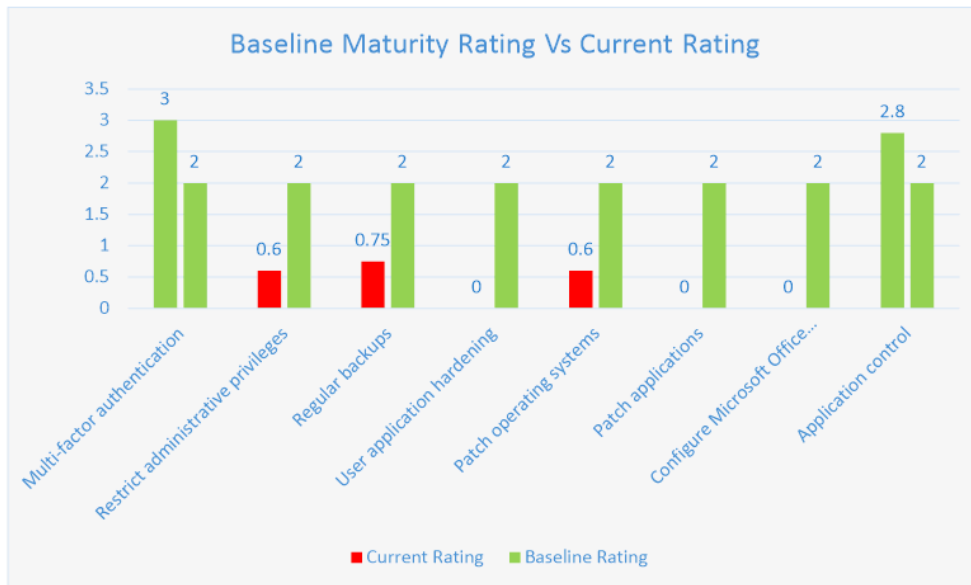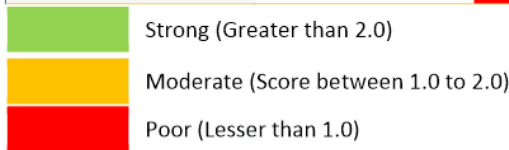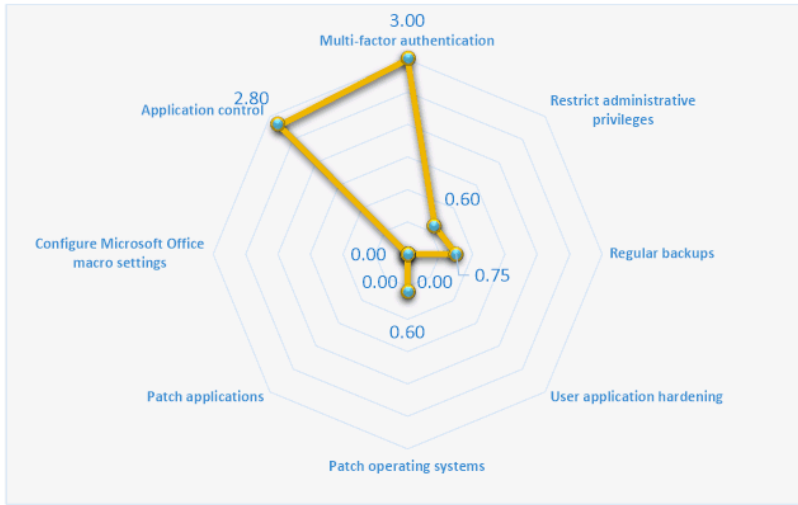
The summary of findings for the Essential 8 controls are documented below:

Control	Current State Summary of Findings	Maturity Level
Restrict Administrator Privileges	• Privileged accounts can still login to the unprivileged Operating environments • Privileged accounts (excluding privileged service accounts) are not prevented from accessing the internet, email and web services. • Windows Defender Credential Guard and Windows • Privileged access to systems and applications are not automatically disabled after 45 days of inactivity. • There is no unique Credentials for local administrator accounts and service accounts • Privileged access to systems and applications are not automatically disabled after 12 months • Defender Remote Credential Guard are not enabled.	0.60
Regular Backups	• There is no Business Continuity Plan • Testing of backups are not conducted periodically • Restoration of backups not done • Unprivileged accounts are not prevented from modifying or deleting backups. • Users with Privileged accounts can still access backups	0.75
User Application Hardening	• There is no documented hardening guidelines • Web browsers are not configured to block web advertisements • PowerShell is not configured to use Constrained Language Mode • PDF software is not blocked from creating child processes. • Blocked PowerShell script executions are logged • Microsoft Office is not blocked from creating executable content. • Microsoft Office is not blocked from injecting code into other processes. • Web browser, Microsoft Office and PDF software security settings cannot be changed by users	0
Patch operating systems	• There is no vulnerability scanner to identify the missing patches or security vulnerabilities	0.6

ASD Essential 8 Controls
maturity assessment |
September 2022 | 8

Control	Current State Summary of Findings	Maturity Level
Patch Applications	• Controls pertaining to patching of applications are not implemented nor appropriate risk management practices are enabled in the environment • Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are not applied within two weeks of release, or within 48 hours if an exploit exists. • A vulnerability scanner is not used at least daily to identify missing patches or updates for security • Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are not applied within two weeks of release, or within 48 hours if an exploit exists, this is covered only as a part of Patch Cycle	0
Configure Microsoft Office Macros	• There are no Microsoft Macros settings enabled throughout the Organisation	0
Application Control	• Application whitelisting control is not implemented throughout the Organisation	2.8

Road to Improvement

The figure below shows at a high level, the activities that the Council is recommended to carry out to transition from their current state of maturity on the Essential 8 controls to the baseline maturity. At this point we are only considering those controls, where the maturity level is less than 2.

Regular Backups
- A full restoration testing needs to be performed at least annually
- Access control for Backup data needs to be clearly defined

User application hardening
- Web browser configuration
- MS Office configuration changes
- PDF software configuration
- Log PowerShell script executions

Patch Application and Patch OS
- Vulnerability scanner shall be implemented to identify the missing patches
- The latest release, or the previous release, of operating systems shall be updated for workstations, servers and network devices.

Current overall maturity – 0.97

Target overall maturity – 2.0

Restrict Administrator Privileges
- Appropriate controls to restrict Privilege accounts shall be implemented
- Use and changes to privilege accounts shall be logged
- Privileged and unprivileged accounts shall be clearly distinguished

Macro Settings
- Meet all the requirements as per the Application control requirement of ASD Essential 8

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Following are detailed recommendations for improvements to the controls, whose maturity is less than 2.0. Implementation of the recommendations will elevate the maturity levels for the controls to 2.0

Control	Recommendation(s) for mitigation	Risk(s) if mitigation is not applied
Multi-factor Authentication (MFA)	• All the critical and non-critical systems shall be implemented with MFA	• Minimal detection of forced attempts by unauthorised users to bypass multi-factor authentication controls
Restrict Administrator Privileges	• Ensure that Privileged account users cannot logon to unprivileged Operating environments • Enable Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. • Use of privileged access and changes to Privileged access shall be logged • Privileged users shall use separate privileged and unprivileged operating environments. • Privileged accounts (excluding local administrator accounts) should not be able to logon to unprivileged operating environments. • SIEM Solution can be considered for	• Inactive privileged access accounts increase threat footprint • Minimal detection for attempt to execute system utilities by inactive privileged accounts • Minimal detection of unaccounted for changes to privileged system accounts
User Application Hardening	• Web browsers are configured so they do not process web advertisements from the internet • Microsoft Office is blocked from creating child processes • Microsoft Office is blocked from creating executable content • Microsoft Office is blocked from injecting code into other processes • Microsoft Office is configured to prevent activation of OLE packages • PDF software is blocked from creating child processes • ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented • Blocked PowerShell script executions are logged	• Increased threat footprint as a result of increased number of vulnerabilities introduced by applications and processes that are not required to be run by the business
Patch Application	• Patches, updates or vendor mitigations for security vulnerabilities in other applications shall be applied within two weeks of release. • vulnerability scanner shall be used at least daily to identify missing patches or updates for security vulnerabilities • Controls pertaining to patching of applications shall be implemented • Vulnerability scanner shall be used to implemented to identify the missing patches and Security vulnerabilities • All the End of Life applications shall be removed from the environment	• Weak controls on the application patching increases the vulnerabilities on your software and applications that are susceptible to cyber-attacks • Vulnerabilities in the OS and applications software such as web browsers and document readers or in PC and adapter firmware can allow threat actors to run malware and gain a foothold on the network

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Control	Recommendation(s) for mitigation	Risk(s) if mitigation is not applied
Application Control	• Application whitelisting controls shall be implemented or appropriate risk management practices shall be enabled • The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients • Allowed and blocked executions on workstations and internet-facing servers shall be logged • Microsoft's 'recommended block rules' and 'recommended driver block rules' shall be implemented • Allowed and blocked executions on workstations and internet-facing servers are logged	• Increased threat footprint by expansion of privileges to execute utilities using standard user profiles • Minimal detection for execution of blocked utilities on workstations and internet facing servers
Patch Operating Systems	• Vulnerability scanners shall be used to identify the missing patches and security vulnerabilities • Latest release, or the previous release, of operating systems shall be used for workstations, servers and network devices.	• Poor patch management can leave an organisation's data exposed, subjecting them to malware and ransomware attacks where data is hijacked unless a ransom is paid
Configure Microsoft Office macro settings	• Allowed and blocked Microsoft Office macro executions are not logged • Microsoft Office's list of trusted publishers are not followed • Allowed and blocked Microsoft Office macro executions are not logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected • Evidence of the control implementation could not be verified as the snap shot of the console was not shared by the council	• Utilisation of vulnerabilities in unsigned and unverified macros for weakening the security and launching malicious applications

Data Breach Insights from 2021

- Australian organisations have seen close to a 25 percent increase in data breaches resulting from ransomware incidents according to the latest report from the Office of the Australian Information Commissioner (OAIC)

- The latest Notifiable Data Breaches Report showed the agency received 446 data breach notifications from January to June 2021, 43 percent of which were from cyber security incidents.

- Data breaches arising from ransomware incidents in particular increased by 24 percent, up from 37 notifications last reporting period to 46.

- There was a 10% increase in the number of claims notified to insurers between 1 July 2021 – 31 December 2021, compared to the previous six months.

ASD Essential 8 Controls
maturity assessment |
September 2022 | 13
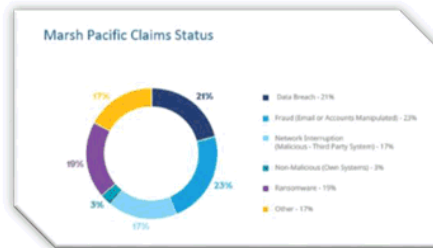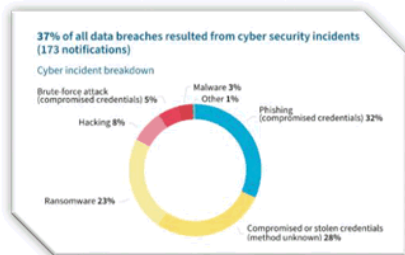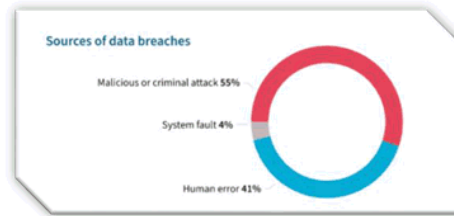
NEXT STEPS

Following the ASD 8 essential assessment, these are the next steps that we recommend:

- Defining the risk profile for each control as a result of inadequacies in the current implementation of controls. This will help the council in drafting the right mitigation strategies and minimise the probability of Cyber Security breach / data breach that can be caused by internal or external threats

- Define Data Classification policy document to identify the critical and non-critical data and strengthen the controls to protect the critical / confidential data handled by the council

- Create a roadmap, which is essentially a statement on the improvement areas and plan of action for implementation of the improvement areas. This is where the organisation will review the risk statements and categorise them into the relevant risk actions i.e., accept, mitigate, transfer or avoid

- Create the strategy for implementation of the improvements for which risk mitigation is selected as the action in the roadmap. The strategy takes into consideration the budget available for implementation of the controls and prioritises the actions accordingly over a time frame of 12-18 months

- Development of cyber incident response plans and cybersecurity awareness training for employees of the council to minimise possibilities of unintentional internal attacks through negligence or unawareness

![LGIS Mutual Services logo]

Level 3, 170 Railway Parade
West Leederville WA 6007
T: +61 8 9483 8888

lgiswa.com.au

Title	Information and Cyber Security
Policy Number (Governance Purpose)	

Policy Type

Administration

Policy Purpose

To prevent, where possible, cyber security incidents, and to safeguard, as far as is reasonably practicable, the Information and Communications Technology (ICT) assets of the City of Cockburn (the City).

To ensure that the City has business continuity to reduce business damage by minimising the impact of, and increase resilience to, cyber security incidents.

To achieve best practice in ICT risk management by implementing an Information Security Management Framework (ISMF) which has been developed in accordance with the requirements of Standards Australia AS ISO/IEC 270001:2013 *Information technology - Security Techniques - Information security management systems — Requirements.*

This policy applies to all City staff, suppliers and contractors across all City sites and assets.

Policy Statement

The City is committed to developing, maintaining and continually improving an ISMF to ensure that:

(1)   Legal, contractual and regulatory requirements are met -

  1. The Executive Team and Senior Management Team will promote a culture within the City of awareness and active implementation of this policy; and
  2. The Executive Team and Senior Management Team will ensure that all staff, suppliers and contractors have the required knowledge and training in the areas needed to uphold these requirements.

(2)   Confidentiality, integrity and availability of information is protected -

  1. The City will implement controls over systems and processes to prevent unauthorised access to City data and ICT assets; and
  2. All City staff must at all times maintain the confidentiality, integrity and availability of information by only allowing those authorised City staff, suppliers and contractors to view it, to take necessary steps to prevent unauthorised editing of information and to have information available when required.

(3)   Business Continuity Plans (BCP) are developed, maintained and tested to ensure that the City is able to deliver critical services to the Community during a business disruptive incident -

[1]

Title	Information and Cyber Security
Policy Number (Governance Purpose)	

(4)   All suspected breaches of information security are reported and investigated -

1. All City staff, suppliers and contractors must report to their Line Managers any breaches, or suspected breaches of information security; and
2. The City's Information Services business unit must investigate any reported breaches, or suspected breaches of information security to continually improve the resilience, redundancy, rapid recovery of the City's ISMF.

(5)   Where appropriate, the City applies other security controls to the City's ICT assets on an ad hoc basis as required, to ensure the confidentiality, integrity and availability of information and where existing controls are deemed insufficient.

Strategic Link:	Strategic Community Plan – Key Objective 'Leading & Listening'
Category:	Business, Economy & Technology
Lead Business Unit:	Information Services
Public Consultation: (Yes or No)	No
Adoption Date: (Governance Purpose Only)	10 September 2019
Next Review Due: (Governance Purpose Only)	September 2021
ECM Doc Set ID: (Governance Purpose Only)	8564383

Document Set ID: 8564383
Version: 3, Version Date: 02/10/2019

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023
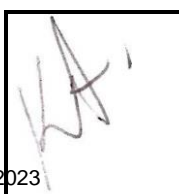
11.3 Operations

11.3.1   (2023/MINUTE NO 0008) Henderson Waste Recovery Park Annual Department of Water and Environmental Regulation (DWER) Report

Responsible Executive	Chief Operations Officer
Author	Waste Services Manager
Attachments	1. Henderson Waste Recovery Park - Annual Report ⇩

Officer Recommendation/Committee Recommendation

MOVED Cr T Dewan SECONDED Cr P Corke

That Council:

(1)   RECEIVES the Henderson Waste Recovery Park Annual Report to the Department of Water and Environmental Regulation.

CARRIED 5/0

Background

The Henderson Waste Recovery Park (HWRP) operates under a licence (L9159/2018/1) issued by the Department of Water and Environmental Regulation (DWER).

Section 36 of the licence states: The licence holder must submit to the CEO Department of Water and Environmental Regulation (DWER) an Annual Environmental Report within 28 days after the end of the annual period.

The annual period is defined as the 12-month period commencing from 2 March until 1 March of the year immediately following.

The report is to include:

- Condition 5.2.1 - Summary of any failure or malfunction of any pollution control equipment and any environmental incidents that have occurred during the annual period, and any action taken
- Condition 5.2.1 - Surveyed Topographic Contour Map depicting the area of the planned footprint, including cross sections for cut slopes, filled areas and unexcavated areas
- Condition 3.6.1 -Waste input and output data (including rejected loads)
- Condition 3.7.1 - Process monitoring
- Condition 3.8.1 - Monitoring of Ambient Groundwater Quality
- Condition 5.1.3 - Compliance Annual Audit Report
- Condition 5.1.4 - Compliant Summary
- Condition IR5 - Submit a Geotechnical Report.

The report and attachments were signed by the A/Chief Executive Officer and electronically submitted to DWER on 20 March 2023.

Note, the annual report is being presented to the May 2023 ARC as the report was not finalised until after the closing date for agenda items to the 16 March 2023 ARC.

Submission

N/A

Report

The 2022/23 Annual Report, attached, has been prepared in accordance with the proforma issued by the DWER.

Responses to each of the City's licence conditions have been detailed along with all supporting documentation being issued with the report.

Key highlights of the report include:

1. Compliance with Licence
2. Approval to bury quarantine waste current
3. 182,092 tonnes of waste received (30% increase on 2021/22)
4. 21,109 diverted from landfill
5. Two complaints received
6. 2 Bushfire crossed into the Site causing facility closure and evacuation.
7. Household Hazardous Waste removal:
    a) 91.8 tonnes of chemicals and paint
    b) 27.72 tonnes of gas bottles.

Strategic Plans/Policy Implications

Environmental Responsibility
A leader in environmental management that enhances and sustainably manages our local natural areas and resources.
• Sustainable resource management including waste, water and energy.

Budget/Financial Implications

The report was prepared by officers within the Waste Service Unit with costs associated with external reports covered under operational budgets.

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

As the report has been issued to the Department of Water and Environmental Regulations, there is a low risk the City's licence will be revoked should Council not adopt the recommendation.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

2022/23 Annual Report

Henderson Waste Recovery Park

Licence No. L9159/2018/1

Author: Lyall Davieson
Waste Manager

March 2023

Cover Picture: Fire in the Medium Strip to Rockingham Road Outside the Entrance to the Henderson Waste Recovery Park

TABLE OF CONTENTS

2

Government of **Western Australia**
Department of **Environment Regulation**

EXECUTIVE SUMMARY

In the reporting period beginning 2 March 2022 to 1 March 2023 the Henderson Waste Recovery Park (HWRP) received 182,092 tonnes. This is a 30% increase from the previous reporting period.. Products and materials totalling 21,109 tonnes were diverted from landfill which equates to 11.6% of the total tonnes received. Recycled metals are still attracting reasonable spot market prices.

The weighbridge was recalibrated on 11 March 2023 to ensure compliance with State regulatory authorities.

Two complaints were received during the reporting period. One related to dust and the other related to odour and dust.

4 fires occurred in the reporting period. 2 occurred as a result of bushfires from adjoining land and two from separate waste delivered to the Transfer Station and the active face of Cell 7.

Cleanaway removed Household Hazardous Waste from the Hazardous Waste Store as follows;
91.8 Tonnes of chemicals and paints and
27.72 Tonnes of gas bottles in the reporting period.

The Site's Commonwealth Department Agriculture Water and Environment approval to bury quarantine waste is current.

The City continues to ensure that the HWRP operates beyond best practice principles and exceeds the requirements of the DWER Licence.

INTRODUCTION

The Henderson Waste Recovery Park (HWRP) accepts MSW, C&I, C&D, Inert waste annually.

The City of Cockburn has operated the HWRP in Rockingham Road, Wattleup since 1990, when the first lined landfill cell was constructed in WA. Cells One, Two and Three were completed in the 90's, Cell Four was commissioned in 2000, and Cell Five in Feb 2004. Cell Six was commissioned in October 2007 and Cell Seven in December 2012. The City capped Cell Six in 2020 and Cell 7 is the active landfill cell.

The HWRP provides an essential service to the Kwinana Industrial strip and many other commercial and domestic users.

The HWRP has developed its capacity to remove reusable product from the waste stream and will continue to divert waste from landfill to meet the City's Sustainability Targets and the State Waste Strategy goals.

3

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Government of **Western Australia**
Department of **Environment Regulation**

SITE OPERATIONS SUMMARY

Refrigerant degassing was contracted to Workpower during the reporting period and will continue for the foreseeable future.

The City has a Memorandum of Understanding under the State Government's Household Hazardous Waste (HHW) Program. Under this program, Cleanaway removed 118.86 tonnes of Household Hazardous Waste from the Hazardous Waste Store as follows;

      91.9   Tonnes of chemicals and paints and
      27.72 Tonnes of gas bottles in the reporting period.

Department of Agriculture, Water and Environment representative conducted another successful annual audit of the quarantine burial process during the reporting period on 22 November 2022. The Site's Commonwealth Department Agriculture Water and Environment approval to bury quarantine waste is current.

The City has contracted the processing of its garden and greenwaste waste to convert the material to compost.

Site boundaries and internal buffers have not changed.

During the reporting period, 2 fire incidents were recorded in the Incident Register due to Site operations. The first fire occurred on 23/3/2022 on Cell 7 with City staff extinguishing the fire. No damage was caused. The second fire occurred on the Transfer Station on 21/1/23 with no damaged reported.
2 fires entered the HWRP as a result of bushfires from adjoining land. DFES was called to assist on both occasions. The Park was closed and evacuated. The fires occurred on 17/12/23and 16/2/23 with no damage to the landfill infrastructure.

In 2022/23 the City awarded the tender for the bulk earthworks for the Cockburn Resource Recovery Precinct upon receipt of the Development Application.

The HWRP operates under an Environmental Management Plan that is central to our Operation Manual. The HWRP management and staff operate under the City's Waste Strategy 2020-2030, approved DWER Waste Plan and the Sustainability Policy. These documents detail requirements for improved environmental outcomes and beyond best practice waste management principles along with committing the City to further improve its renewable energy targets and environmental sustainability initiatives.

DWER LICENCED PREMISES REPORTING RESPONSIBILITY

The City of Cockburn currently holds a DWER Licence No. L9159/2018/1, which expires on the 22 October 2031. Under 5.2.1 of this Licence, the City is required to submit an Annual Report to the CEO of the Department of Water and Environmental Regulation within 28 calendar days after the end of the annual period

4

Government of **Western Australia**
Department of **Environment Regulation**

The report is to include:

- Condition 5.2.1. Summary of any failure or malfunction of any pollution control equipment and any environmental incidents that have occurred during the annual period and action taken - Refer Water Pollution Control Conditions
- Condition 5.2.1 Surveyed Topographical contour map depicting the area of planned footprint including cross sections for cut slopes, filled area and un-excavated area - See Attached
- Condition 3.6.1 – Waste input and output data.
- Condition 3.7.1 – Process Monitoring
- Condition 3.8.1– Monitoring of Ambient Groundwater Quality.
- Condition 5.1.3 – Compliance Annual Audit Report
- Condition 5.1.4 - Complaint Summary
- Condition IR5 –   Submit a Geotechnical Report

Table 5.2.1

Water Pollution Control Conditions

The Post Winter 2022 Groundwater Monitoring Report for the Site is sent as attachment to this Annual Report. The Post Summer 2022 Groundwater Monitoring Report for the site was not completed at the time this report was prepared. This Report will be forwarded to the DWER when it becomes available.

Surveyed Topographical Contour Map

The surveyed topographic contour map depicting the area of filled landfill cells are attached in the submission package to this Report as a DWG, PFD and Word files.

Condition 3.6.1

Waste Input and Output Data

- Refer to the drop box for spreadsheets detailing the Landfill Reports covering the period March 2022 – February 2023.
- Special Waste Type One. The Asbestos Logbook is available at the HWRP office and details all asbestos waste placements. The asbestos disposal area is a single column in Cell Seven. The GPS coordinates are consistent with every burial.
  Northwest Corner S=32 degrees 09 .911. E= 115 degrees 47.943.
  Northeast Corner S =32 degrees 09.912. E= 115 degrees 47.971.
  Southwest Corner S= 32 degrees 09.922 E= 115 degrees 47.941.
  Southeast Corner S=32 degrees 09 .926 E= 115 degrees 47.970.
  73.38 tonnes were received and buried in the reporting period.
- Special Waste Type Two. The Clinical Waste Logbook is available at the HWRP and identifies the GPS location of each individual burial. 1,330.5 Tonnes were landfilled in the reporting period.

5

Government of **Western Australia**
Department of **Environment Regulation**

- Quarantine Waste. The Quarantine Burial Logbook is available at the HWRP and identifies the GPS location of each individual burial. 224.3 tonnes were landfilled in the reporting period.
- Waste Leaving the Site. The Rejected Loads Register recorded seven loads during the reporting period were rejected by the Weighbridge Officers as non-compliant. One rejected load was a biosecurity load without a booking. The other 6 were domestic customers who failed to correctly wrap asbestos. This Register is available in the HWRP Weighbridge Office

Condition 3.7.1

Process Monitoring

Mulched Greenwaste Windrows

Currently greenwaste is removed from the domestic waste stream only and stockpiled onsite until it is mulched.
The stockpiles of greenwaste and mulch have not exceeded the respective 2000m^3 or 6000m^3 limits as specified in the Licence Conditions.
Greenwaste is stored in a manner that minimises fire risk.

Small greenwaste stockpiles remain on site (< 100m^3) for consumption, free of charge, by HWRP domestic users. Any large mulch stockpile is monitored throughout the holding period for temperature and recorded in the Greenwaste Logbook according to the Licence Conditions.

Leachate Monitoring

Refer to Ground Water Monitoring Report in the submission package.

Condition 3.8.1

Monitoring of Ambient Groundwater Quality

The October Post Winter 2022 Ground Water Monitoring Reports is included in the submission package. The Post Summer 2023 Groundwater Monitoring Report will be forwarded to the DWER when completed. These Reports were undertaken by Strategen JBS&G for the HWRP under the WALGA Landfill Groundwater and Contaminated Site Tender.

Condition 5.1.3
Compliance Annual Audit Report.

Refer to Section B.

Condition 5.1.4
Complaint Summary

6

Government of **Western Australia**
Department of **Environment Regulation**

Two complaints were received during the reporting period. One related to dust and one related to Dust and odour. All complaints were noted in the Complaints Register during the reporting period.

Condition IR5
Geotechnical Report

Refer to the submission package.

Schedule 2: Reporting & notification forms

These forms are provided for the proponent to report monitoring and other data required by the Licence. They can be requested in an electronic format.

ANNUAL AUDIT COMPLIANCE REPORT PROFORMA

SECTION A

LICENCE DETAILS

Licence Number:	**L9159/2018/1**	Licence File Number: **DER2018/001433**
Company Name:	**CITY OF COCKBURN**	ABN: **27471341209**
Trading as:	**CITY OF COCKBURN**	
Reporting period:	**2/03/21 to 1/03/22**	

STATEMENT OF COMPLIANCE WITH LICENCE CONDITIONS

1. Were all conditions of the Licence complied with within the reporting period? (please tick the appropriate box)

           Yes ☐ Please proceed to Section C

           No ☑ Please proceed to Section B

Each page must be initialled by the person(s) who signs Section C of this Annual Audit Compliance Report (AACR).

1. Were all conditions of the Licence complied with within the reporting period? (please tick the appropriate box)

           Yes ☐ Please proceed to Section C

           No ☑ Please proceed to Section B

Initial: ……………………………………..

7

Government of **Western Australia**
Department of **Environment Regulation**

SECTION B

ANNUAL AUDIT COMPLIANCE REPORT FORM
Environmental Protection Act 1986, Part V Division 3

Once completed, please submit this form either via email to info@dwer.wa.gov.au, or to the below postal address:

> Department of Water and Environmental Regulation
> Locked Bag 10
> Joondalup DC WA 6919

Section A – Licence details			
Licence number:	L9159	Licence file number:	DER2018/001433
Licence holder name:	City of Cockburn		
Trading as:	Henderson Waste Recovery Park		
ACN:			
Registered business address:			
Reporting period:	2/3/2022 **to** 1/3/2023		

Section B – Statement of compliance with licence conditions
Did you comply with all of your licence conditions during the reporting period? (please tick the appropriate box)
☐ Yes – please complete: • section C;   • section D (if required); and   • sign the declaration in Section F.
☒ No – please complete: • section C;   • section D (if required);   • section E; and   • sign the declaration in Section F.

Initial: …………………………………….

8

77 of 146

Government of **Western Australia**
Department of **Environment Regulation**

Audit Compliance Reports
Fire Incident 21 January 2023

Section C – Statement of actual production	
Provide the actual production quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual production quantity**
64	140,176 tonnes

Section D – Statement of actual Part 2 waste discharge quantity	
Provide the actual Part 2 waste discharge quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual Part 2 waste discharge quantity**
64	5,000Lts

Section E – Details of non-compliance with licence condition			
Please use a separate page for each condition with which the licence holder was non-compliant at a time during the reporting period.			
Condition no:	General Site Management Condition 7	Date(s) of non-compliance:	21 January 2023
Details of non-compliance:			
A small fire ignited in the Transfer Station from the delivery of residential waste.			

What was the actual (or suspected) environmental impact of the non-compliance?

NOTE – please attach maps or diagrams to provide insight into the precise location of where the non-compliance took place.

Nil the fire occurred on the profiling hardstand
Cause (or suspected cause) of non-compliance:
Unknown
Action taken to mitigate any adverse effects of non-compliance and prevent recurrence of the non-compliance:
The water cannon on the water cart was deployed and sand was then dumped on the extinguished waste.
Was this non-compliance previously reported to DWER?
☒ No

☐ Reported to DWER verbally	Date: / /
☐ Reported to DWER in writing	Date:

Initial: …………………………………….

9

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Government of **Western Australia**
Department of **Environment Regulation**

Section F – Declaration

I / We declare that the information in this Annual Audit Compliance Report is true and correct and is not false or misleading in a material particular[i].

I / We consent to the Annual Audit Compliance Report being published on the Department of Water and Environmental Regulation's (DWER) website.

Signature[ii]:		Signature:	
Name: (printed)	Daniel Arndt	Name: (printed)	
Position:	Acting CEO	Position:	
Date:		Date:	

Fire Incident March 2022

Section C – Statement of actual production	
Provide the actual production quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual production quantity**
64	140,176 tonnes

Section D – Statement of actual Part 2 waste discharge quantity	
Provide the actual Part 2 waste discharge quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual Part 2 waste discharge quantity**
64	5,000lts

Initial: …………………………………….

10

Government of **Western Australia**
Department of **Environment Regulation**

Section E – Details of non-compliance with licence condition			
Please use a separate page for each condition with which the licence holder was non-compliant at a time during the reporting period.			
Condition no:	General Site Management Condition 7	Date(s) of non-compliance:	23 March 2022
Details of non-compliance:			
Fire ignited on Cell 7			
What was the actual (or suspected) environmental impact of the non-compliance?			
NOTE – please attach maps or diagrams to provide insight into the precise location of where the non-compliance took place.			
Burning of waste.			
Cause (or suspected cause) of non-compliance:			
Unknown			
Action taken to mitigate any adverse effects of non-compliance and prevent recurrence of the non-compliance:			
Burn material was soaked with the water cannon, covered with sand, spread out and resoaked.			
Was this non-compliance previously reported to DWER?			
☒ No			
☐ Reported to DWER verbally		Date: / /	
☐ Reported to DWER in writing		Date:	

Initial: …………………………………….

11

Government of **Western Australia**
Department of **Environment Regulation**

Section F – Declaration			
I / We declare that the information in this Annual Audit Compliance Report is true and correct and is not false or misleading in a material particular[iii].			
I / We consent to the Annual Audit Compliance Report being published on the Department of Water and Environmental Regulation's (DWER) website.			
Signature[iv]:		Signature:	
Name: (printed)	Daniel Arndt	Name: (printed)	
Position:	Acting CEO	Position:	
Date:		Date:	

Complaint 1 - Dust and Odour - 1 March 2022

Section C – Statement of actual production	
Provide the actual production quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual production quantity**
64	140,176 tonnes

Section D – Statement of actual Part 2 waste discharge quantity	
Provide the actual Part 2 waste discharge quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual Part 2 waste discharge quantity**
64	50,000Lts

Initial: …………………………………..

12

Government of **Western Australia**
Department of **Environment Regulation**

Section E – Details of non-compliance with licence condition

Please use a separate page for each condition with which the licence holder was non-compliant at a time during the reporting period.

Condition no:	General Site Management Condition 8 and 10	Date(s) of non-compliance:	1 March 2022

Details of non-compliance:

Odour from Cell 7 and the landfilling operations and dust from reshaping batters

What was the actual (or suspected) environmental impact of the non-compliance?

NOTE – please attach maps or diagrams to provide insight into the precise location of where the non-compliance took place.

Odour and dust extended beyond the premises boundary

Cause (or suspected cause) of non-compliance:

Landfill operations and through reshaping of batters

Action taken to mitigate any adverse effects of non-compliance and prevent recurrence of the non-compliance:

A less dusty cover material was applied and the reshaping of the batter work ceased in strong wind conditions

Was this non-compliance previously reported to DWER?

☒ No

| ☐ Reported to DWER verbally | Date: /   / |
| ☐ Reported to DWER in writing | Date: |

Section F – Declaration

I / We declare that the information in this Annual Audit Compliance Report is true and correct and is not false or misleading in a material particular[v].

I / We consent to the Annual Audit Compliance Report being published on the Department of Water and Environmental Regulation's (DWER) website.

Signature[vi]:		Signature:	
Name: (printed)	Daniel Arndt	Name: (printed)	
Position:	Acting CEO	Position:	
Date:		Date:	
Seal (if signing under seal):			

Initial: …………………………………….

13

Government of **Western Australia**
Department of **Environment Regulation**

Complaint 2 – Dust -31 March 2022

Section C – Statement of actual production	
Provide the actual production quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual production quantity**
64	140,176 tonnes

Section D – Statement of actual Part 2 waste discharge quantity	
Provide the actual Part 2 waste discharge quantity for this reporting period. Supporting documentation is to be attached.	
Prescribed premises category	**Actual Part 2 waste discharge quantity**
64	Odour discharge across the boundary to be zero

Section E – Details of non-compliance with licence condition			
Please use a separate page for each condition with which the licence holder was non-compliant at a time during the reporting period.			
Condition no:	General Site Management Condition 8	Date(s) of non-compliance:	31 March 2022

Details of non-compliance:
Dust reported outside the boundary premises.

What was the actual (or suspected) environmental impact of the non-compliance?
NOTE – please attach maps or diagrams to provide insight into the precise location of where the non-compliance took place.
Dust extended west to adjoining property due to strong easterly winds over several weeks.

Cause (or suspected cause) of non-compliance:
Hot dry conditions and strong easterly winds over several weeks.

Action taken to mitigate any adverse effects of non-compliance and prevent recurrence of the non-compliance:
Ongoing surveillance of covered landfill areas and deployment of an additional water cart.

Was this non-compliance previously reported to DWER?	
☒ No	
☐ Reported to DWER verbally	Date: / /
☐ Reported to DWER in writing	Date: / /

Initial: …………………………………..

14

Government of **Western Australia**
Department of **Environment Regulation**

Section F – Declaration			
I / We declare that the information in this Annual Audit Compliance Report is true and correct and is not false or misleading in a material particular[vii]. I / We consent to the Annual Audit Compliance Report being published on the Department of Water and Environmental Regulation's (DWER) website.			
Signature[viii]:		Signature:	
Name: (printed)	Daniel Arndt	Name: (printed)	
Position:	Acting CEO	Position:	
Date:		Date:	

SECTION C

SIGNATURE AND CERTIFICATION

This Annual Audit Compliance Report (AACR) may only be signed by a person(s) with legal authority to sign it. The ways in which the AACR must be signed and certified, and the people who may sign the statement, are set out below.

Please tick the box next to the category that describes how this AACR is being signed. If you are uncertain about who is entitled to sign or which category to tick, please contact the licensing officer for your premises.

If the licence holder is		The Annual Audit Compliance Report must be signed and certified:
An individual	☐	by the individual licence holder, or
	☐	by a person approved in writing by the Chief Executive Officer of the Department of Environment Regulation to sign on the licensee's behalf.
A firm or other unincorporated company	☐	by the principal executive officer of the licensee; or
	☐	by a person with authority to sign on the licensee's behalf who is approved in writing by the Chief Executive Officer of the Department of Environment Regulation.
A corporation	☐	by affixing the common seal of the licensee in accordance with the *Corporations Act 2001*; or
	☐	by two directors of the licensee; or
	☐	by a director and a company secretary of the licensee, or
	☐	if the licensee is a proprietary company that has a sole director who is also the sole company secretary – by that director, or
	☐	by the principal executive officer of the licensee; or
	☐	

15

Government of **Western Australia**
Department of **Environment Regulation**

		by a person with authority to sign on the licensee's behalf who is approved in writing by the Chief Executive Officer of the Department of Environment Regulation.
A public authority (other than a local government)	☐	by the principal executive officer of the licensee; or
	☐	by a person with authority to sign on the licensee's behalf who is approved in writing by the Chief Executive Officer of the Department of Environment Regulation.
a local government	☐	by the chief executive officer of the licensee; or
	☐	by affixing the seal of the local government.

It is an offence under section 112 of the *Environmental Protection Act 1986* for a person to give information on this form that to their knowledge is false or misleading in a material particular. There is a maximum penalty of $50,000 for an individual or body corporate.

Initial: …………………………………..

I/We declare that the information in this annual audit compliance report is correct and not false or misleading in a material particular.

SIGNATURE: SIGNATURE: _____

NAME: NAME:
(printed) Daniel Arndt   (printed)_____

POSITION: Acting Chief Executive Officer   POSITION: Acting CEO

DATE: ?????? 2023   DATE: _____/_____/_____

_____

[i] It is an offence under section 112 of the *Environmental Protection Act 1986* for a person to give information on this form that to their knowledge is false or misleading in a material particular.
[ii] AACRs can only be signed by the licence holder or an authorised person with the legal authority to sign on behalf of the licence holder.
[iii] It is an offence under section 112 of the *Environmental Protection Act 1986* for a person to give information on this form that to their knowledge is false or misleading in a material particular.
[iv] AACRs can only be signed by the licence holder or an authorised person with the legal authority to sign on behalf of the licence holder.
[v] It is an offence under section 112 of the *Environmental Protection Act 1986* for a person to give information on this form that to their knowledge is false or misleading in a material particular.
[vi] AACRs can only be signed by the licence holder or an authorised person with the legal authority to sign on behalf of the licence holder.
[vii] It is an offence under section 112 of the *Environmental Protection Act 1986* for a person to give information on this form that to their knowledge is false or misleading in a material particular.
[viii] AACRs can only be signed by the licence holder or an authorised person with the legal authority to sign on behalf of the licence holder.

16

11.4 Governance and Strategy

11.4.1   (2023/MINUTE NO 0009) Risk Maturity Assessment - Report

Responsible Executive	Executive Governance and Strategy
Author	Manager Legal and Compliance
Attachments	1. Risk Maturity Review 2023 ⇩

Officer Recommendation/Committee Recommendation
MOVED Cr P Corke SECONDED Cr T Dewan
That Council:

(1)   ACCEPTS the Risk Maturity Assessment Report; and

(2)   RECEIVES annual reporting to the Audit Risk and Compliance Committee, on the Risk Maturity Improvement Plan.

<u>**CARRIED 5/0**</u>

Background

The City set a corporate KPI to undertake a Risk Management Maturity Review by June 2023.

Regulation 17 of the *Local Government (Audit) Regulations 1996* provides that the Chief Executive Officer is to review the appropriateness and effectiveness of a local governments systems and procedures in relation to risk management not less than once every three years.

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

Moore Australia were engaged by the City to complete a broad scope Risk Maturity Review.

The purpose of the external review is to determine the appropriateness and effectiveness of the City's risk management practices, against the Australian Standard AS ISO 31000:2018 Risk Management Guidelines.

The scope of the review included the City's Risk Management Framework, Risk Culture and Risk Management processes.

Submission

N/A

Report

The Report is attached for consideration by the Audit Risk and Compliance Committee (ARC).

The objective of a risk maturity review is to assess an organisation's ability to effectively identify, evaluate, and manage risks across its operations.

The review aims to evaluate the maturity of the organisation's risk management processes and to identify areas where improvements can be made.

A risk maturity review typically involves an assessment of the organisation's risk management framework, policies and procedures and practices as well as an evaluation of the effectiveness of risk management activities, and the alignment of those activities with the organisation's overall strategic objectives.

A risk maturity review may also examine risk culture, risk appetite, risk reporting and communication and the roles and responsibilities of individuals involved in the risk management process.

The ultimate objective is to aid the organisation in developing more robust and effective risk management, which can help better manage risks, protect assets and reputation, and ultimately achieve its strategic objectives.

Moore Australia were engaged to conduct the review. Moore assessed the maturity of the City's Risk Management Framework, the Risk Culture, and the Risk Management process.

Moore Australia have finalised the review report and it is presented to the ARC for review (note: the document is marked draft for the City's input to finalise).

The report has identified the City's maturity in the three areas reviewed to be inadequate.

There are several recommendations in the report and the City's response/actions will form the Project Implementation Plan to address the recommendations (Risk Maturity Improvement Plan).

The Risk Maturity Improvement Plan is presented to the ARC for information only. The actions, owners, and delivery dates may be subject to change

The implementation of the Risk Maturity Improvement Plan is an operational matter, however given the outcomes of the risk maturity review it was deemed prudent to provide assurance to the ARC of the City's response.

A mature risk management framework is one which is characterised by a number of key attributes:

1. A clear understanding of the organisation's risk appetite, tolerance and strategy.
2. An integrated approach to risk management with risk considerations integrated into all aspects of the organisation's decision-making processes.
3. The use of standardised risk management processes and tolls which are consistently applied across the organisation.
4. The use of objective risk assessments to identify, evaluate and prioritise tasks.
5. The implementation of effective risk mitigation strategies, which are regularly monitored and updated as needed.
6. The establishment of a strong risk culture with a shared understanding of the importance of risk management and a commitment to continuous improvement.

As identified in the report, the City has a number of actions to implement in order to work towards being a more mature organisation in its approach to risk management.

The independent Risk Maturity Review highlights the City's areas which need improvement, and the Risk Maturity Improvement Plan identifies the actions to be undertaken.

Reporting on the Risk Maturity Improvement Plan will be presented to the ARC for assurance and transparency.

On 14 April the Council resolved to:

> *"...CONDUCT a briefing session on the topic of the City's Corporate Risk Management Framework and Policy, and its strategic relevance to the City"*

Moore will be presenting to the Elected Members at a future Elected Member Strategic Briefing Forum (EMSBF) on Risk Management, where Elected Members will also have the opportunity to ask questions directly to Moore representatives regarding the Risk Maturity Assessment and Risk Management at the City of Cockburn.

The objective of the Risk Maturity Improvement Plan and the EMSBF for Elected Members is to progress improvements in the City's Risk Maturity and provide assurance to the Elected Members.

Strategic Plans/Policy Implications

Listening & Leading
A community focused, sustainable, accountable and progressive organisation.
• Best practice Governance, partnerships and value for money.
• High quality and effective community engagement and customer service experiences.

Budget/Financial Implications

The FY24 and FY25 budgets include a provision for the implementation of the Risk Maturity Improvement Plan.

Legal Implications

Local Government (Audit) Regulations 1996 r17 CEO to review certain systems and procedures.

Community Consultation

NA

Risk Management Implications

The Risk Maturity Review has identified several areas of improvement in the City's Risk Management Framework, the Risk Culture, and the Risk Management Processes.

The report has benchmarked the City's practices, procedures, framework etc against industry standards and best practices.

This benchmarking helps the City understand its current position and areas of improvement.

The delivery of the Risk Management Improvement Plan will require substantive resources, and some skills which the City cannot meet internally.

The City has to operate accepting some of the areas of concern while the improvement Plan is implemented, which is itself an exercise of determining the City's risk appetite.

Due to the nature of the recommendations from the Risk Maturity Review, it is recommended regularly reporting on the actions and outcomes be presented to the ARC to ensure that improvements are made and sustained over time.

The objective is for the organisation to more effectively manage risk and improve its risk management maturity over time.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

RISK MANAGEMENT MATURITY REVIEW

City of Cockburn

8 May 2023

TABLE OF CONTENTS

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices
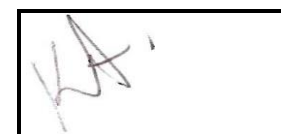
1.　EXECUTIVE SUMMARY

1.1.　Background

The City of Cockburn is a local government in Western Australian. As a local government, the City's Chief Executive Officer ("CEO") is required by *Regulation 17 of the Local Government (Audit) Regulations 1996* to review the appropriateness and effectiveness of the City's systems and procedures in relation to **risk management**, **internal controls**, and **legislative compliance** and to report the outcome to the Audit, Risk and Compliance Committee.

To assess how well the City's current risk management practices are working to ensure the City is ready for the above review, the City requires an independent review of its risk management processes against better practice. Risk Management is a critical part of the First Line of Defence.

This is represented in Figure 1 below.
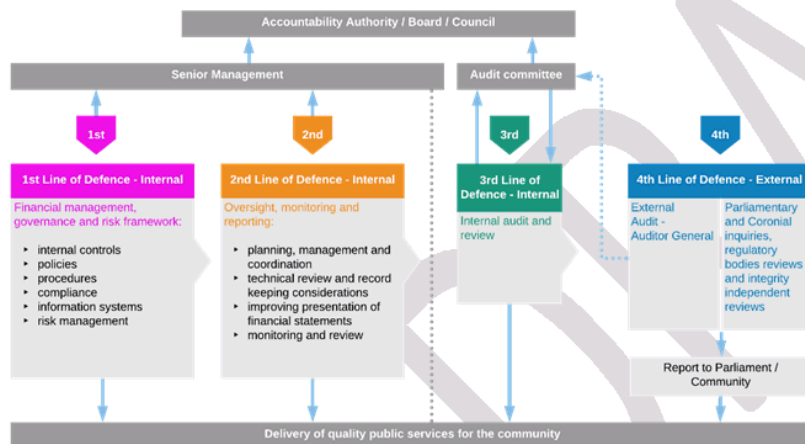
Figure 1: Four Lines of Defence Model. Source: Office of the Auditor General

1.2　Objective and Scope

The objective of the review is to provide the basis for a report by the Chief Executive Officer to the Audit, Risk & Compliance Committee ("ARC") on the appropriateness and effectiveness of the City's risk management practices, against the Australian Standard AS ISO 31000:2018 Risk Management - Guidelines.

The scope of the Risk Management Maturity Review engagement will include:

- **A review of the Risk Management Framework** - The City's approach to risk management, including documentation, review, governance, and compliance with standards;

- **A review of the Risk Culture** - How the culture of the City supports risk management, from clear commitment of the Senior Leadership Team through to reward and recognition programs; and

- **A review of the Risk Management Process** - How the City systematically deploys policies, processes, and procedures to manage risk.

1.3　Approach

The review is to be conducted primarily by applying discussion, observation, and review techniques, concentrating on:

- Entrance meeting with Risk Management Process Owner;

- Holding meetings with relevant stakeholders to understand the current environment, challenges, and opportunities;

- Review of documentation provided during the engagement;

- Exit meeting with Risk Management Process Owner to discuss emerging observations and recommendations;

- Issue of Draft Risk Management Maturity Review Report;

- Receive and incorporate Management feedback; and

- Issue final report to the ARC.

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

1.   EXECUTIVE SUMMARY (CONT.)

1.4   Summary of Work Performed

Moore Australia assessed the risk management using the Local Government Audit Committee Guidelines (2013). This document identifies the key areas of internal controls within a Risk Management Maturity Review. We have also used the Australian Standard AS ISO 31000:2018 Risk Management – Guidelines as better practice.

In our professional judgement, sufficient and appropriate review procedures were completed, and appropriate evidence gathered to support the accuracy of the conclusions reached and contained in this report. As mentioned above, the scope of the review is on the appropriateness and effectiveness of the City's risk management practices.

1.5   Overall Observation

Risk Management is a critical function in the governance of the City. The Council, Audit, Risk and Compliance Committee ("ARC"), Management, Employees, Contractors, Consultants and Volunteers all have a role to play to ensure it is resourced, efficient and effective.

The quantity and nature of the observations and recommendations demonstrate there is considerable room for improvement within Risk Management maturity in the City. There is significant investment of resources and time required to improve the Risk Management Framework, Risk Culture and Risk Management Process. The City may not be able to adequately demonstrate, based on available documentation and existing practice, an effective Risk Management function which requires:

- A robust and strong documentation of risk management and governance framework and policies in the City;

- Regular review and timely update of the risk management and governance documents, as well as the related policies to ensure relevancy to the City's operations and activities;

- A good risk management and governance framework which align to compliance requirements and better practice principles, where fit for purpose for the City;

- Positive culture and strong capability to drive the implementation of risk management activities, regular risk training and awareness;

- Consistent implementation of risk management and governance framework, policies and processes across all levels in the City, Risk management is embedded in the City's culture, environment and processes to ensure it is integrated at all levels;

- Effective risk assessment to review validity of risk profile and monitoring of risk management action plans and comprehensive risk reporting to the SLT, ARC and Council; and

- Systems which are easy to use, reliable, continuity and maintain confidentiality and insight which is gained from the systems to inform decision making.

1.6   Maturity Assessment Model

There are three elements which have been agreed with Management and assessed within the engagement. This includes Risk Management Framework, Risk Culture and Risk Management Process. The definitions have been set out in Table 1 below.

1. Risk Management Framework	The City's approach to risk management, including documentation, review, governance, and compliance with standards
2. Risk Culture	How the culture of the City supports Risk management, from clear commitment of the Senior Leadership Team through to reward and recognition programs
3. Risk Management Process	How the City systematically deploys policies, processes, and procedures to manage risk.

Table 1 Definitions for Risk Management Maturity Model.

1.7   Summary of Observations

Moore Australia has completed a review of the City's Risk Management function. As stated above, there are three areas where we assessed the Risk Management practices. These areas included: **1. Risk Management Framework, 2. Risk Culture, and 3. Risk Management Process.** A summary of the observations is identified in Table 2 below.

Area	High	Medium	Low	Total
1. Risk Management Framework	2	3	1	6
2. Risk Culture	1	2	4	7
3. Risk Management Process	4	9	9	22
Total	7	14	14	35

Table 2: Summary of Observations

The Key Observations and Recommendations are set out in Section 3.2.

MOORE

93 of 146
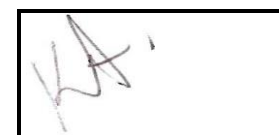
1.   EXECUTIVE SUMMARY (CONT.)

1.8   Summary of Risk Management Maturity Model

We have assessed the Risk Management practices of the City using a maturity model as set out below. See Figure 2 for the Risk Management Maturity Model.

Risk Management Maturity	Level 1 – Inadequate	Level 2 – Acceptable but Requires Development	Level 3 – Effective	Level 4 – Optimal
Risk Management Framework				
Risk Culture				
Risk Management Process				

Figure 2: Overall Risk Management Maturity Model

1.9   Acknowledgement

We have met and / or interviewed key personnel within the City to perform the engagement. We would like to thank the following personnel for their assistance in the review (by division).

Governance & Strategy Division
- Acting Chief Executive Officer;
- Executive Governance & Strategy;
- Risk & Governance Advisor;

Community Services Division
- Chief of Community Services;
- Head of Library & Cultural Services;
- Head of Community Safety & Ranger Services;
- Manager, Recreation Infrastructure and Services;

Finance Division
- Acting CFO;
- Acting Head Finance;
- Head of IT;
- Head of Procurement;

Operations Division
- Chief of Operations;
- Head of Property & Assets;
- Head of Operations and Maintenance;
- Manager, Building Services;

Corporate Affairs
- Executive Corporate Affairs;

People Experience and Transformation Division;
- Acting Executive People Experience and Transformation; and
- Head of Workplace Health and Safety

2. SCOPE AND APPROACH

2.1. Background

Risk management is an integral part of good management practice and an essential element of sound corporate governance. Risk management involves establishing an appropriate framework and culture, and applying a logical and systematic method to identify and manage risks by:

- implementing and communicating an organisational policy;

- balancing risk and opportunity within organisational policies;

- defining the organisation's Risk Appetite and Tolerance to inform decision making;

- training Council Members, ARC Members, Management, and Officers in their risk management, and oversight responsibilities;

- identifying, analysing, evaluating, treating, monitoring, and communicating risks associated with any activity, function or process in a way that will maximise the potential to achieve strategic objectives and minimise risks within Risk Appetite and Tolerance; and

- Risk Management is a critical part of the First Line of Defence.

2.2. Objective and Scope

The objective of the review was to determine the compliance, efficiency, and effectiveness of the Risk Management Framework and its consideration of better practice principles.

The scope of the Risk Management Maturity Review engagement will include:

1. A review of the **Risk Management Framework**. The City's approach to risk management, including documentation, review, governance, and compliance with standards. This includes:

   - a framework expressed in terms that are easy to understand and carry out;

   - well defined processes and policies, which are communicated to the whole organisation and are easy for staff to access; and

   - demonstrated commitment from the Senior Leadership Team.

2. A review of the **Risk Culture**. How the culture of the City supports risk management, from clear commitment of the Senior Leadership Team through to reward and recognition programs. This includes:

- desired values and behaviours defined in key documents and communicated to staff;

- people Leaders acting in line with the values and behaviour and modelling the culture; and

- practices that encourage learning and innovation

3. A review of the **Risk Management Process**. How the City systematically deploys policies, processes, and procedures to manage risk. This includes:

   - transparent risk management processes, which are communicated to the City as a whole and can be easily accessed;

   - risk response planning; and

   - a continuous improvement process that captures lessons learned and makes them available for future projects.

2.3. Summary of Work Performed

Moore Australia assessed the risk management using the Local Government Audit Committee Guidelines (2013). We have also used the Australian Standard AS ISO 31000:2018 Risk Management – Guidelines as better practice.

This document identifies the key areas of internal controls within a Risk Management Maturity Review.

In our professional judgement, sufficient and appropriate review procedures were completed, and appropriate evidence gathered to support the accuracy of the conclusions reached and contained in this report.

The overall scope of the engagement has excluded certain areas and so this report needs to be read in conjunction with that exclusion.

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3. OBSERVATIONS AND RECOMMENDATIONS

3.1 Risk Management Overall Conclusion

Overall, there is 'Inadequate' Risk Management Framework, Risk Culture and Risk Management Process within the City.

The City may not be able to adequately demonstrate, based on available documentation and existing practice, an effective Risk Management function.

3.2 Key Observations 7

Risk Management Framework

The Risk Management Framework is assessed as being 'Inadequate'. There are improvement opportunities identified which include:

1. **Risk Management Policy** – There is a Risk Management Policy however we identified a few improvement opportunities:

   - Risk Appetite was referenced in the Enterprise Risk Management Framework but not in the Risk Management Policy;

   - Governance structure was not defined in the Risk Management Policy. This includes:

     o Roles and responsibilities of Risk Officer, relevant departments, and governing committee in managing risks; and

     o Reporting lines.

   - Focus is currently on business continuity and risk management but not on other key risks currently managed by the City e.g., Strategic Risk, Reputation Risk, Financial, Compliance Risk, Operational Risk including fraud and corruption risks, Project Risks and OSH.

2. **Enterprise Risk Management Framework ("RMF")** – We identified the following improvement opportunities in the RMF:

   - The RMF is dated July 2021. It is due for its next review in December 2022, and this has not been performed;

   - Some of the contents in the RMF were outdated e.g.; it still refers to the Audit and Strategic Finance Committee instead the ARC;

   - We noted that not all risk owners interviewed, particularly the non-ExCo members are aware of the RMF. Some of the feedbacks from the risk owners are that RMF should be simplified, less legislative and focus on what it means to the employees and risk owners; and

   - We noted that majority of the Risk Management Action Plans have not been performed as planned in the RMF which is a non-compliance issue noted.

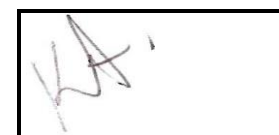| Action	Description	Responsibility	Timing	Moore Australia Comments
Strategic Risk Management Review	Strategic risk workshops with the key deliverable of a strategic risk register for the City, to identify high level key strategic risks associated with the City's external environment, stakeholders, strategic direction and systemic organisational issues.	Executive Committee (coordinated by Governance Services)	Every 4 years in conjunction with the SCP review	In April 2019, the City's Executive team conducted a series of risk profiling workshops to review its Risk registers and risk appetite statement. However, no evidence of workshop provided.
Risk Maturity Review	Maturity review to measure and test Risk Management culture and assess appropriateness and effectiveness of the City's systems and procedures in relation to risk management, internal controls and legislative compliance.	Managers (coordinated by Governance Executive Committee, Business / Service Unit Heads & All)	Biennially	Previous Risk Management Maturity Assessment was performed by the RiskWest in 2018 and due in October 2020. Last Reg 17 performed in November 2020 (triennial review). Due in Nov 2023.

◤◣ MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.　OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2　Key Observations (cont.)

Risk Management Framework (cont.)

Action	Description	Responsibility	Timing	Moore Australia Comments
Review Risk Management Framework	Review the currency and effectiveness of Council's RMF.	Council to adopt (review to be coordinated by Governance Services)	Biennially	RMF approved in July 2021 and due for next review in Dec 2022.
Build robust contingency services to ensure the protection of Council assets and services	Annual test and review of Council Business Continuity & Crisis Management Program.	Governance Services	Annually	Business Continuity Exercise was last performed by the RiskWest in 2017.
Review Operational Risk Registers	Review risks and controls contained in Council's corporate risk register and identify new or emerging risks.	All Managers (risk owners) to complete review (review to be facilitated by Governance Services)	Annually – presented to A&SFC	Risk & Governance Advisor will review the risk register in the RMSS regularly and conducts risk chats with the risk owners and risk managers. Review is also performed online via RMSS in February - March every year, however, there was no discussion note documented.
Risk Controls Assurance Review	Targeted control review to rate and confirm the effectiveness for controls contained in the operational risk register.	Governance Services	Annually – presented to the November Executive Committee Meeting	As informed by the City, this may be an outdated action plan.
Include risk treatment plans in Operational Plan	Ensure that actions required by risk treatment plans are incorporated into the Operational Plan.	All Managers	Every year in conjunction with Operational Plan development / review	As informed by the City, no Operational Plan is in place.
Risk assessments for projects / initiatives in accordance with the project methodology	Conduct risk assessments as required for new or altered activities, processes or events.	Relevant Manager / Risk Owner / Project	Prior to deciding to proceed with new project	As informed by the City, the risk assessments conducted for new or altered activities, processes, or events prior to deciding to proceed with new project are not part of the RMSS and independently covered by the Project Portfolio Management (PPM).
Operational Plan	Identify key risks that may impact on objectives as well as strategies and controls in place (or proposed) to manage those risks.	Managers / Risk Owners (overseen by Governance Services)	Annually	As informed by the City, no Operational Plan is in place.
Staff Performance Review	Ensure risk management performance of managers is assessed on a regular basis.	Manager, Human Resources	Annually	• No risk management included in recognition and risk award programs. • No managers performance review specifically addressing risk management.

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Framework (cont.)

3.   **Risk Appetite Statement** – We identified the following improvement opportunities in the Risk Appetite Statement:

- Did not include all risks such as:
  - Strategic risks – alignment to achieve strategic objectives and strategic community plans; and
  - Governance – implementation of governance control framework.
- There was no definition of risk appetite levels such as no, very low, low, moderate, high;
- No consideration of the costs to reach the Risk Appetite within the Risk Appetite Statement in the RMF as having low appetites comes as a cost;
- There was no reference to Risk Appetite in the management of risks and comparison to residual risks. This is where effective risk management takes place to determine whether the City's risks are within or outside the approved risk appetite; We noted that not all risk owners interviewed, particularly the non- ExCo members are aware of the Risk Appetite;
- The Risk Appetite is not quantified or articulated to be an effective tool to compare the Residual Risk, Strategic Plan, or Risk Register. It needs to be quantified so it can be compared to Residual Risk and Treatment Actions identified to reduce Residual Risk to within Risk Appetite; and
- No process to ensure any risks which sit outside the defined risk appetite are escalated to the ARC or Council for review and decision-making.

4.   **Risk Tolerance Statement –** There is currently no Risk Tolerance Statement developed to set the degree of variance from the City's Risk Appetite that the City is willing to tolerate.

5.   **Strategic Risk Management Plan –** We noted that the Risk Management Action Plans are currently documented in the RMF. However, there was no Strategic Risk Management Strategy (i.e., more than one year) or Risk Management Plan (i.e., annual plan) in place.

6.   **Risk Management Procedures Manual** – There are RMSS User Guides which sets out guidelines as to how to use the system to identify and assess risks, evaluate the control and update of risk actions. These are not a procedures manual for how risk management is embedded within the City and does not underpin the Risk Management Framework.

Management Comment

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Framework (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
1.	Review and revise the **Risk Management Policy** to: • Make reference to the Risk Appetite Statement in the RMF; • Include governance structure in managing risks in the City. This includes the high-level roles and responsibilities of Risk Officer, relevant departments, and governing committee in managing risks, as well as the reporting lines and structure; • Focus on other key risks currently managed by the City e.g., Strategic Risk, Reputation Risk, Financial, Compliance Risk, Operational Risk including fraud and corruption risks, Project Risks and OSH; and • Reflect better practice principles and ensure the policy is implemented, reviewed and approved on a timely basis.	Medium	A risk appetite statement and risk management governance to be developed and added to the Risk Management Policy. The risk policy will be reviewed to include governance structure in managing risks in the City. Improvements to risk reporting to the Audit Risk and Compliance Committee to improve focus on key risks. Biennial review of the Risk Management Policy	Governance & Strategy	Q2 FY 2023-2024
2.	Review and update the **RMF** to ensure that contents are relevant and reflect the current practice and processes. Ensure that RMF is easy to understand and focus on the key tasks and processes that employees need to carry out. This will encourage employees to adhere and adopt the framework. Ensure that the Risk Management Action Plans included in the RMF are effectively tracked, implemented and periodically reported to the ARC and Council. Any delays should be reported to the ARC and Council for review and decision-making.	High	Complete a comprehensive review of the Risk Management Framework adopting recommendations from the Risk Maturity Review.	Governance & Strategy	Q2 FY 2023-2024

MOORE

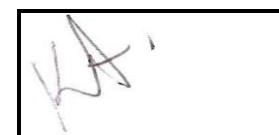| Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)
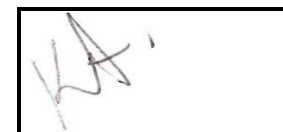
3.2   Key Observations (cont.)

Risk Management Framework (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
3.	Enhance the **Risk Appetite Statement** to: • Include all other key risks managed by the City including Strategic and Governance risks; • Clearly definite the appetite levels and consider costs factor when defining the Risk Appetite; • Monitor and report on a Risk Appetite within the City and then consider these in relation to the Residual Risk rating and whether the City are within the Risk Appetite; and • Escalate any risks which sit outside the defined risk appetite to the ARC or Council for review and decision-making. Clearly communicate the revised Risk Appetite Statement to all employee for reference.	Medium	Adoption of a risk appetite statement for the City of Cockburn will include costs consideration which addresses the elements identified in the Risk Maturity Review.	Governance & Strategy	Q3 FY 2023-2024
4.	Develop **Risk Tolerance** which sets the degree of variance from the City's risk appetite that the City is willing to tolerate and clearly communicate to all employee. This includes specifying the circumstances which are allowable for each risk tolerance level.	Low	Develop the risk tolerance statement for the City of Cockburn to set the degree of variance from the City's risk appetite that the City is willing to tolerate.	Governance & Strategy	Q2 FY 2024-2025
5.	• Develop a **Risk Management Strategy** and **Risk Management Plan** and review the strategy and plan at least every 3 years and annually respectively, or when material risks are identified. Consider moving the Risk Management Action Plans in the RMF to the Risk Management Strategy and Risk Management Plan; and	High	Develop a City of Cockburn Risk Management Strategy, which considers the City's Strategic Community Plan.	Governance & Strategy	Q2 FY 2023-2024
	• Ensure that the actions in the strategy and plan are effectively monitored, timely closed and periodically reported to the ARC and	High	Incorporate appropriate reporting to the ARC on the Risk Management	Governance & Strategy	Q2 FY 2023-2024

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

Risk Management Framework (cont.)

	Council. Any delays should be reported to the ARC and Council for review and decision-making.	■	Strategy and Risk Management Plan. Develop and implement a Risk Management plan.		
6.	Develop and approve a **Risk Management Procedure** which are effective for staff to perform risk management responsibilities.	Medium	Replace guidelines with a risk management procedure to support staff in performing their risk management responsibilities.	Governance & Strategy	Q4 FY 2023-2024

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Culture

The Risk Culture is assessed as being *'Inadequate'*. There are improvement opportunities identified which include:

7.   **Audit, Risk and Risk Committee ("ARC") Term of Reference** – The ARC plays a key role in the oversight of risk management function and sets the "tone at the top" and overall risk culture of the City together with the Council and SLT. We understand it was approved by Council on 13 October 2022 and it also does not appear to align with better practice principles and does not have a Version Control table including endorsement and approval of the TOR . The ARC's Terms of Reference requires improvements:

a)   Roles of responsibilities

- Roles of responsibilities to review the effectiveness of system of internal control for the City and not just limited to and in the context of Regulation 17 only; and

- Reference to Risk Appetite and RMF, including oversight of identification and management of emerging risks.

b)   Memberships

- CEO and employees are currently not a member of the ARC. However, the ARC Terms of Reference did not preclude the CEO and Officers of the City to be ARC members; and

- Payment to ARC External Members was not mentioned by the City.

c)   Meetings

- There was no meeting quorum stated in the ARC's TOR. As per the TOR, the Committee will comprise a minimum of four (4) Members, who shall be appointed by Council, and includes one (1) independent. We noted the following inconsistencies in members' attendance:

ARC Meeting	Attendees
19 May 2022	4 members (non-independent)
28 July 2022	4 members and 1 independent member
21 Sep 2022	3 members and 1 independent member
7 Dec 2022	3 members

- Conduct of meetings is too explicit and could lead to non-compliance (e.g. The Committee shall be held in person at 6:00pm to 7:00pm or at 7:30 to 8:30pm on rotating basis with the other 3 Committees); and

- Ability to meet remotely and proxies not included.

d)   Delegation

- As per the ARC TOR, the ARC will be delegated the authority to meet with appointed external auditor. Meeting the auditor is not be a delegation item as the ARC does not need any delegation to meet with the auditors. The TOR should specify the requirement for ARC to meet with both appointed external auditor and internal auditor privately.

e)   Reporting - Process and minimum timeline for Circulation of agenda papers.

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

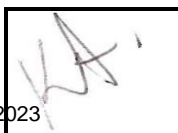**Risk Culture (cont.)**

f)   In addition to the above, the following were not included in the ARC TOR to reflect the better practice principles:

- Performance Review of the ARC including KPI's;
- Awareness and Training of ARC Members;
- Use of experts, when required;
- Access to budget, if required with approval of CEO;
- Conflicts of interest management; and
- Requirement for periodic review of the TOR

8.   **Resources** – There was no assessment of the adequacy of the resources for Risk Management.

9.   **Budget** – No budget was specifically allocated for risk management. A budget includes training and the use of experts when identified as a need by the City.

10.   **Job Descriptions ("JD")** - The following observations were noted:

- No evidence that the position descriptions of employees include responsibility for identification and monitoring of risks, although this was mentioned as one of the measurement controls in the Risk Management Indicators;
- Some of the Specific Accountabilities / Statement of Duties outlined in the Job Descriptions for Risk and Governance Advisor appears to be not being performed:
   - Develop, manage and review Council's ongoing Risk Management Strategy; and
   - Undertake risk audits and reporting regime to Executive and Audit and Strategic Finance Committee, as required.

11.   **Recognition and reward programs -** Risk management was not included in recognition and reward programs, although this was mentioned as one of the measurement controls in the Risk Management Indicators.

12.   **Risk Experts –** Risk Experts are recommended to complement in house resources for complex and sensitive risk management e.g. redefining / development of Risk Appetite and Risk Tolerance levels and ensuring that risks are being managed within Risk Appetite and Risk Tolerance.

13.   **Awareness and Training –** The awareness and training observations are as follows:

- There was no specific and structured risk management training session performed on an annual basis or on ad-hoc basis for employees and SLT to provide an overview of the RMF, as required by the RMF. There was also no formal Risk Management Training Calendar in place. We noted that training performed in 2022 were mainly relating to the functionality of the new RMSS Version 16 and training materials provided are mainly Cheat Sheet on how to use the RMSS. In addition, there were BCM workshop conducted in October and November 2022. We are not able to sight to any attendance records and training register maintained;

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3. OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2 Key Observations (cont.)

Risk Culture (cont.)

- Most of the risk owners interviewed recommend a relaunch of RMF and a formal and structured risk management training to brief them on their roles and responsibilities in risk management and risk assessment process. This is a recommendation in a further observation;

- No risk trainings performed for ARC. There were 2 risk trainings conducted for SLT on 2 operational risks in Jun 2022 (i.e. Hazard and child safety risks) and 1-hour RMSS training provided to the SLT. No attendance records and register were maintained;

- The Elected Member Training for 2021/2022 and 2022/2023 published on City website and showed that:

  o There was no training for risk management, internal control framework including fraud / corruption, misconduct and WHS; and

  o Limited training on risk topics such as Risk landscape / insight, ESG, cyber security risk etc .

- The City does not currently consider Risk Management upon induction and termination of employees. Provision of awareness and training on Risk management matters such as identification of Risk Owners, fraud and corruption, PID training etc. was not performed upon commencement and termination so that new ones can be appointed.

Management Comment

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
7.	• Review the **ARC's Terms of Reference** to include recommended improvements and align with better practice principles, including reviewing the performance of the ARC on a regular basis to ensure responsibilities are being performed; and	Medium	Annually review the ARC Terms of Reference.	Governance & Strategy	Q1 FY 2023-2024
	• Ensure the role and responsibility of the ARC is being performed efficiently and effectively each year in compliance with the revised Terms and Reference.		Annually review the ARC performance.	Governance & Strategy	Q4 FY 2023-2024
8.	Perform assessment of the adequacy of the **resources for Risk Management**. This will ensure sufficient and quality resources to implement roboust risk management process and drive strong risk management cultures and internal control environment to meet legislative compliance requirements and better practice principles.	Medium	Review current risk management resourcing for the City and make recommendations where required.	Governance & Strategy	Q3 FY 2023-2024

MOORE

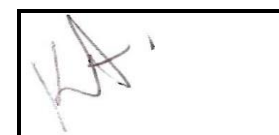| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

Risk Culture (cont.)

- Most of the risk owners interviewed recommend a relaunch of RMF and a formal and structured risk management training to brief them on their roles and responsibilities in risk management and risk assessment process. This is a recommendation in a further observation;

- No risk trainings performed for ARC. There were 2 risk trainings conducted for SLT on 2 operational risks in Jun 2022 (i.e. Hazard and child safety risks) and 1-hour RMSS training provided to the SLT. No attendance records and register were maintained;

- The Elected Member Training for 2021/2022 and 2022/2023 published on City website and showed that:
  - There was no training for risk management, internal control framework including fraud / corruption, misconduct and WHS; and
  - Limited training on risk topics such as Risk landscape / insight, ESG, cyber security risk etc .

- The City does not currently consider Risk Management upon induction and termination of employees. Provision of awareness and training on Risk management matters such as identification of Risk Owners, fraud and corruption, PID training etc. was not performed upon commencement and termination so that new ones can be appointed.

| 9. | Allocate budget specifically for risk management activities. This includes risk management training and the use of experts when identified as a need by the City. | Low | Review current risk management budget for the City and make recommendations where required. | Governance & Strategy | Q2 FY 2024-2025 |

3. OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2 Key Observations (cont.)

Risk Culture (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
10.	• Include the responsibility for identification and monitoring of risks in the **position descriptions** of employees. This will ensure accountability and that they are aware of their roles and responsibilities in risk management; and	Low	Review all organisation PDs and include responsibility for identification and monitoring of risks.	People Experience & Transformation	Q4 FY 2023-2024
	• Review the Specific Accountabilities / Statement of Duties outlined in the **JD for Risk and Governance Advisor** to assess whether they are still relevant. If yes, ensure compliance with the JD. Otherwise, update the JD to reflect current roles and requirements.		Review Risk and Governance Advisor PD	Governance & Strategy	Q1 FY 2023-2024
11.	Include risk management in the **recognition and reward programs** to drive and encourage good risk management culture.	Low	Incorporate reward and recognition actions for risk management.	People Experience & Transformation	Q1 FY 2023-2024

MOORE

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

Risk Culture (cont.)					
12.	Consider the need for a **Risk Expert** in the redefinement of Risk Appetite and development of Risk Tolerance levels. Also to ensure that risks are being managed within Risk Appetite and Risk Tolerance.	Low	Develop City of Cockburn Risk Appetite and Risk Tolerance statement.	Governance & Strategy	Q4 FY 2023-2024
13.	• Develop, maintain and implement a **formal approach to risk management training** for employees and SLT within the City including Future Training Program. This should include briefing on RMF, roles and responsibilities in risk management, risk assessment process and risk topics for risk awareness. Ensure retention of training material, and maintenance of attendance records for quality assurance and audit purposes; • Design a structured training for risk management and internal control for the Elected Members. This includes fraud / corruption, misconduct and WHS Training and risk topics such as risk landscape / insight, ESG, cyber security risk etc; and • Include Risk Management upon induction and termination of employees.	High	Develop and deliver a formal training program for all staff, with annual reviews and delivery. Program delivery to be audited.	Governance & Strategy	Q2 FY 2023-2024
			Develop and deliver a cyber security risk formal training program for all staff.	Finance	Q2 FY 2023-2024
			Develop and deliver a formal training program for Elected members, with annual reviews and delivery. Program delivery to be audited.	Governance & Strategy	Q3 FY 2023-2024
			Develop and deliver a formal training program for all staff, as part of induction for new employees, with annual reviews and delivery. Program delivery to be audited.	People Experience & Transformation	Q4 FY 2023-2024

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3. OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2 Key Observations (cont.)

Risk Management Process

The Risk Management Process is assessed as being '*Inadequate*'. There are improvement opportunities identified which include:

14. **Risk Identification and Risk Register –** The observations about the Strategic Risk Register and Operational Risk Register are as follows:

- No regular strategic risk workshops conducted to identify and update key strategic risks associated with the City's external environment, stakeholders, strategic direction and systemic organisational issues. We were also unable to sight to the evidence of the last strategic workshop performed in 2019;

- As at September 2022 ARC meeting, there were 7 Strategic Risks and 272 Operational Risks included in the City's Risk Register and does not adequately identify succinctly operational risks to enable them to be managed effectively or efficiently. Interviews with risk owners and review of the Risk Register revealed that there are too many risks and duplicated risks noted in the Operational Risk Register. There is also very limited input from the risk owners on the risk descriptions. Hence, risk owners are not agreeable with some of the risk descriptions written. Risk Taxonomy is not expanded to include other risk categories such as Reputation Risk, Financial Risk, Compliance Risk, Fraud and Corruption Risk, Project Risks;

- Some of the key stakeholders interviewed are not fully aware of the Strategic Risks and Operational Risks recorded in the RMSS under their division's purview. No regular risk discussions or risk reports provided to the SLT for their review. Risk owners are currently not trained, and they are not familiar with the risk assessment process. Very limited information provided in the RMF to guide staff on risk identification process;

- As represented by the risk owners, the last risk workshop was performed more than 18 months ago and was very high-level. Subsequently, there was no risk assessment or risk workshop conducted for each division to review all the risks collectively in the Risk Register. At present, risk owners will update the status of a particular action plan upon receiving notification from RMSS and will not focus on reviewing the risk descriptions of other risks. Hence, some of the risk descriptions may be obsolete and require updates;

- There are various risk register templates used for projects, programs, events, hazard assessments, cyber security assessments and WHS which are kept offline and not kept within RMSS. We understand that the RMSS system is currently not able to support these risk assessments. We were not provided the evidence that risks were identified and action plans were monitored and reported to ensure timely closure. The City uses the TechnologyOne Project Portfolio Management ("PPM") online solution for managing high value projects. Projects risks are registered in PPM and some projects risks, usually associated with strategic finance are captured in RMSS. Other assessments are manually recorded on paper and / or in spreadsheets;

- Risk events with low likelihood or high consequence ("black swan events") were not identified so that scenario planning can be implemented to ensure that the City can recover quickly from major disruptions and outages; and

- Both the Strategic Risk Register and the Operational Risk Register do not provide a comparison of the Residual Risk Rating to Risk Appetite and Risk Tolerance.

MOORE

Quick Search	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3. OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2 Key Observations (cont.)

Risk Management Process

15. **Controls identification and effectiveness, and Treatment Actions Plans**

- Currently, there is no testing performed on the effectiveness of controls and treatment action plans provided; and

- As per RMF, the CEO, Divisional Chiefs and Divisional Executives monitor substantial risks and treatment implementation as part of their normal Executive Committee meeting agenda item with specific attention to be given to risks that meet certain criteria (i.e. Risk of High or Extreme level, Risks with an Inadequate Existing Control Rating, a Consequence Rating of Catastrophic; and a Likelihood Rating of Almost Certain). However, we are not able to sight to the evidence that this has been conducted. Subsequently, we were informed that there was no standing item in relation to risk included in the Agenda of the Executive Committee.

16. **Risk Reporting to the SLT, ARC and Council**

- Composition of Operational risks for reporting is not effective. Only 13 Operational Risks categorised as '*substantial*' and above were reported, with no further breakdown or details or analysis provided on the remaining 259 risks (e.g. type of risks, trend of risk etc.,);

- No reporting and escalation of risks which sit outside the defined risk appetite to the ARC and Council for review and decision-making;

- Deep dive was performed on Cybersecurity, harassment and bullying and WHS. This should be done on other key risks on a rotation basis;

- The City has reported 3 notifiable incidents to WorkSafe WA but limited information was provided to the ARC;

- Tabling of OAG reports to the ARC in September 2022 i.e. Information Security Report, OAG Fraud Report and self-assessment. However, no actions clearly identified with timeframes;

- There is no comprehensive reporting of the Risk Management activities to the SLT, Audit and Risk Committee or Council (e.g. status of Risk Management Action plans and Risk Management Indicators as outlined in the RMF); and

- Statements included in the ARC minutes without authority and assessment done i.e. "The report confirms the City has appropriate and effective systems to manage risk aligned to standard AS ISO 31000:2018 Risk Management Guidelines".

17. **Risk Mangement and Safety Systems ("RMSS")** – The following observations were noted in RMSS:

- During the RMSS demo, we sighted the Overdue Actions Report and noted that the report was not accurate as it captures actions which are already closed. We understand that there may be flaw in the system and the system is not user-friendly as there are some limitations in the system e.g. RMSS currently doesn't reflect the changes in organisation structure. i.e. any change of risk owner / manager will have to be updated manually in the system; and

- All the risk owners interviewed confirmed that RMSS is not user-friendly, not intuitive and doesn't encourage user's engagement. E.g. The RMSS notification requires the risk owners to update a particular action plan but it's not visible which risk the action plan is related to.

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

18. **Assurance Map –** There was no Assurance Map within the City which maps the Strategic Risks of the City to the various assurance activities which have been performed over recent times and which are then identified to inform the Straregic Internal Audit Plan.

19. **Access to Risk Manager –** There is no direct access to the Risk Manager by Council, Management, Staff, Contractors and Volunteers. This is a key role for the City there should be direct access to raise safety hazards, additional risks, discuss risk mitigation strategies, seek risk experts, advice or training. This may be via an e-mail address such as risk@cockburn.wa.gov.au.

20. **Information and Cyber Security**

     *   The Information and Cyber Security Policy adopted 10 September 2019, outdated and overdue for next review in September 2021;

     *   The Information and Cyber Security Policy is too high-level lack of the following information;

          o   Roles and responsibility of staff and relevant department and teams in managing and mitigating cyber security risk and threats;

          o   Acceptable usage of IT system and resources, including internet usage;

          o   Access control and access management policy e.g., password management, system access, creation of accounts commensurate with job requirements;

          o   E-mail and communication policy;

          o   ICT Hardware acquisition, handling and disposal;

     *   The ISO 27001 Information security management gap analysis and assessment performed by Cyber CX in December 2021 was not presented to the ARC. The report was presented to the CFO and no evidence that action plans were being tracked and resolved by IT department. The next assessment will be performed by end of 2023 and it's important that the City ensures alignment to the ISO 27001 requirements and include cyber security consideration specifically for projects; and

     *   There was no IT Security Breach Register within the City. As represented by the City, there was no IT data security breach received to-date.

21. **ICT Strategic Plan** - The following observations were noted:

     *   Information Services Strategy Refresh 2018-2020 was dated 12 Aug 2020, outdated and currently being reviewed by the IT Team; and

     *   It outlines the list of projects according to the priorities (Tier 1 – 3) but with no clear timeline assigned.
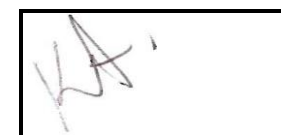
MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

3.　OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2　Key Observations (cont.)

Risk Management Process (cont.)

22.　**Business Continuity, Emergency Management, Incident Management and Crisis Management** –The suite of documents are in various stages of development, none are current, approved, tested or key stakeholders adequately trained. Some specific observations are identified below:

a)　**Business Continuity Plan ("BCP") and Incident Management ("IM"):**

- Draft BCP dated November 2022 and not approved. It did not include key elements and make reference to standards and better practice e.g. ISO standards; and

- The incident scenario in the draft BCP should be expanded to include other potential emergency events and incidents e.g. fire, chemical spills, bomb threats, electrical outages, cyber-attacks, security breaches, medial events and pandemics. Currently, there are emergency evacuation plan for unexpected incident such as fire, injuries, bomb threats, armed confrontations and natural disasters but not the incident management plan and detailed BCP.

b)　**Crisis Management Plan ("CMP"):**

- Crisis Management Plan and Crisis Communication Plan are outdated and currently being reviewed by the external BCM consultant;

- Crisis Management Plan last revised Oct 2017, outdated and overdue for review 20 July 2017; and

- Crisis Communications Plan not dated, no version control table and no approval details.

c)　**Emergency Management Plan ("EMP"):**

- Emergency Management Plan last revised Aug 2015, outdated and overdue for review July 2016. No approval details; and

- No evidence of testing or training.

d)　**Disaster Recovery Plan ("DRP"):**

- Disaster Recovery Design Document – DR Infrastructure dated 4 Jun 2014, outdated and next review not stated. No approval details;

- Records Services – Disaster Recovery Plan July 2014 dated 30 Sep 2003, last revised on 18/09/2020 and next review not stated; and

- Both documents did not include key elements and make reference to standards and better practice.

e)　**Business Continuity Management ("BCM") exercise and testing:**

- No recent testing performed for BCP, IM, CMP, EMP or DRP. Last review was performed by RiskWest Management Consultants on 28 March 2017;

- No evidence of implementation of recommendations arising from the RiskWest Business Continuity Exercise Report;

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

23. **Privacy Breach Register** - There was no **Privacy Breach Register** within the City. As represented by the City, there was no privacy breach received to-date;

24. **Public Information Disclosure ("PID")**;

- There is a PID Statement, but this is not a formal policy. Thus, no version control date, approval details and City's branding;

- The PID officer contact in Public Sector Commission ("PSC") PID Directory is Bernadette Pinto, Governance Officer. However, as per the City's website, the PID Officers are James Ngoroyemoto and Don Green which does not match the PID Directory;

- No PID Procedures in place;

25. **Complaint Management**;

- Compliments, Feedback and Complaints Policy ("Policy") dated 16 March 2021 and due for next review in March 2023;

- The following inconsistencies were noted;

  ○ The Policy requires complaints about employees must initially be directed to the (CEO) for attention. The Complaint Handling Procedures require complaints about employees to be directed to the supervisor or the Manager Human Resources as appropriate;

  ○ The Corporate Governance Framework requires the City to provide resolution or an interim response within five (5) working days, unless otherwise discussed with the complainant. The Complaint Handling Procedures requires the City to acknowledge e-mail or written request within five (5) or seven (7) working days respectively;

- Both Policy and Procedures state that the City complies with the Australian Standard Guidelines and the Ombudsman Western Australia Guidelines, but no evidence of assessment;

- Complaint Register;

  ○ No resolution dates recorded in the Complaint Register for tracking and monitoring purposes;

  ○ The register did not include better practice metrics to efficiently and effectively manage the complaints and to monitor and report this to the ARC;

26. **Freedom of Information**;

- There is an Accessible-Information-Statement-2022-2023 in the City's website (dated 5 Dec 2022), but this is not a formal policy. Thus, no version control with approval details;

- No FOI Procedures in place;

27. **Work Health and Safety** - No version control table to outline the adoption date and next review due and no WHS Procedures; and

28. There was no **Register of Hazardous Material** maintained by the City to reflect properties under the control of the City which may contain hazardous materials such as asbestos, and if associated risks have been adequately treated.

MOORE

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

29.   **Fraud and Corruption** – The following are the observations about the Fraud and Corruption Control.

- There is a Fraud Misconduct Control and Resilience Policy dated 10 June 2021, but reference to the old standards (Australian Standard AS8001-2008 Fraud and Corruption Control) and ASFC. The policy also made reference to the Fraud and Misconduct Control and Resilience Framework dated 13 Aug 2021;

- No Fraud and Corruption Control Plan and procedures;

- No Fraud Incident Register; and

- No other fraud training conducted apart from the fraud training conducted by LGIS on 19 & 26 November 2020. No attendance records and register were maintained.

30.   **Key Performance Indicators ("KPI")** - The RMF identifies Risk Mangement Indicators to measure performance of the Risk Management function. There was no evidence that assessment has been performed to assess the achievement of the KPIs. We noted that some of the current controls included under measurements were not implemented and in place (.e.g. Risk management included in Job descriptions, Risk management is included in recognition and reward programs, Organisation wide risk appetite and tolerance has been documented, approved and available to all staff, Assuramce map).

31.   **Risk Management Process Review** - Previous Risk Management Maturity Assessment was performed by the RiskWest in 2018 and due in October 2020. No evidence that the key actions / recommendations arising from RiskWest's review of the risk management framework in 2018 have been tracked or implemented.

32.   **CEO's Triennial Review For Risk Management, Internal Control and Legislative Compliance** was performed on 19 Nov 2020. However, we noted that only good audit committee practices in monitoring internal control and risk management programs were included, with no recommendation for improvement.

33.   **Surveys** – There was no survey performed to measure the performance of the Risk Management function.

34.   **Data Analytics –** Data analytics has not been considered for use in reporting risk management activities. Data analytics can be a very powerful tool to identify risk areas for Management to focus their limited resources for maximum benefit.

35.   **Better Practice Principles** – There is no comparison of the Risk Management Framework to better practice principles to identify continuous improvement opportunities.
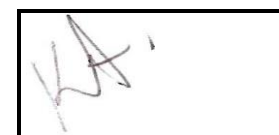
Management Comment

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
14.	Improve the **Risk Identification process and Risk Register:**	High			
	• Conduct regular strategic risk workshops with Executive Committee to identify and update key strategic risks and maintain records of workshops conducted;		Deliver and implement a program for regular workshops with Exco on Risk Management (strategic risks) at the City of Cockburn.	Governance & Strategy	Q4 FY 2023-2024
	• Consider the possibility of merging the Operational Risks for effective risk management and expanding the Risk Taxonomy to include other risk categories such as Reputation Risk, Financial Risk, Compliance Risk, Fraud and Corruption Risk, Project Risks. This will ensure that majority of the risks are not combined as Operational Risks;		Expand risk taxonomy to include these risk categories • Reputational risk • Financial risk • Compliance risk • Fraud and corruption risk • Project Risks.	Governance & Strategy	Q4 FY2023-2024
	• Conduct regular risk workshops with each division, at least half yearly to collectively validate and update the Strategic Risk Register and Operational Risk Registers maintained in the RMSS. During the risk workshop, there should be active engagement with risk owners to review and update the risk descriptions, controls and risk mitigation action plans. Duplicated risks should be merged, and obsolete risks should be removed;		Develop and facilitate a program for half yearly risk management workshops with Divisions at the City.	Governance & Strategy	Q4 FY 2023-2024
	• Update the RMF to include more detailed process to provide guidance to the employees on risk identification process. E.g., How are risks identified, who will review the registers to ensure new or emerging risks are identified and no duplication of risks;		Ensure employees are appropriately informed to seek guidance on risk identification through training.	Governance & Strategy	Q4 FY 2023-2024

MOORE

Page | 24

113 of 146

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

Risk Management Process (cont.)

• Minimise offline risk registers to ensure that various risk register templates used for projects, programs, events, hazard assessments cyber security assessments and WHS are kept within RMSS risk registers. This will ensure centralised recording of risk profile. If the current RMSS is not able to support these assessments, explore using a single platform or system to capture all other assessments;		Adopt a record management practice which complies with the City's record keeping practices and ensures a central repository of all risks.	Governance & Strategy	Q4 FY 2023-2024
• Perform risk assessment for projects, programs, events, hazard, cyber, WHS and ensure action plans identified are monitored and reported to ensure timely closure;		Perform risk assessments for projects, programs, events and hazards, ensuring action plans are monitored and reported to ensure timely closure.	Governance & Strategy	Q4 FY 2023-2024
• Identify the risks events with low likelihood or high consequence ("black swan events"). Implement scenario planning to ensure that the City can recover quickly from major disruptions / outages and setbacks; and		Identify risks with low likelihood or high consequence and implement planning for such risk events	Governance & Strategy	Q4 FY 2023-2024
• Ensure both the Strategic Risk Register and the Operational Risk Register compare the residual risks to Risk Appetite and Risk Tolerance;		Ensure both the Strategic Risk Register and the Operational Risk Register compare the residual risks to Risk Appetite and Risk Tolerance.	Governance & Strategy	Q2 FY 2023-2024

MOORE

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
15.	• Perform random testing on the effectiveness of **controls and treatment action plans** provided. This will ensure controls identified and action plans provided are effectively implemented to mitigate the risks; and	Medium	Ensure random testing of effectiveness of controls is undertaken to determine whether mitigating actions are effective.	Governance & Strategy	Q2 FY 2024-2025
	• Include risk management as one of the standing items in the Agenda of the Executive Committee. Document the evidence of monitoring process performed by the CEO, Divisional Chiefs and Divisional Executives on substantial risks and treatment implementation, as per the RMF.		Exco to adopt a standing item on the monthly agenda.	Governance & Strategy	Q2 FY 2023-2024
16.	Enhance the risk reporting to the SLT, ARC and Council to include the following:	High			
	• More breakdowns or analysis on the remaining risks (e.g., type of risks, trend of risk, etc.), in addition to the 'Substantial' and above Operational Risks reported;		Enhance risk reporting to include breakdown or analysis on the remaining risks (e.g., type of risks, trend of risk etc.,), in addition to the 'substantial' and above Operational Risks reported.	Governance & Strategy	Q4 FY 2023-2024
	• Escalation of risks which sit outside the defined risk appetite for review and decision-making;		Define the review and escalation process for those risks which sit outside the defined risk appetite.	Governance & Strategy	Q4 FY 2023-2024
	• Deep dive to be performed and reported on other key risks on rotation basis;		Develop a deep dive reporting schedule for risks (strategic and operational)	Governance & Strategy	Q4 FY 2023-2024

MOORE

| Quick Search | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

Risk Management Process (cont.)

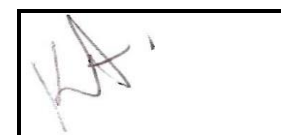|		Risk Rating	Agreed Action	Responsible Owner	Action Date
	• More comprehensive reporting including notifiable incidents to WorkSafe WA, OAG reports, with actions clearly identified with timeframes;	(red)	Develop and implement comprehensive reporting procedure of notifiable incidents.	Governance & Strategy/People Experience & Transformation	Q4 FY 2023-2024
		(red)	Develop and implement comprehensive reporting procedure of OAG reports.	Governance & Strategy	Q4 FY 2023-2024
	• Include a summary of the Risk Management activities as a standard Agenda Paper for SLT, Audit and Risk Committee and / or Council meetings on a regular basis to discuss current, new, emerging risks, status of Risk Management Action plans and Risk Management Indicators, Risk Management Annual Work Plan etc.; and	(red)	Develop reporting framework for regular risk reporting to SLT.	Governance & Strategy	Q4 FY 2023-2024
	• Only include accurate statements in the ARC minutes after assessment done.	(red)	Review all ARC reports for accuracy to remove instances of inaccurate reporting to ARC.	Governance & Strategy	Q4 FY 2023-2024
17.	Discuss with the **RMSS** service provider to explore options to address the system flaw and system limitations. This will ensure that the risk system is user-friendly and providing a good user experience to the system administrator, risk owners and managers. Provide regular training to the risk owners to provide support and guidance on how to use the system.	Medium	Conduct a system suitability analysis and include recommendations.	Governance & Strategy	Q4 FY 2024-2025

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
18.	Develop an Assurance Map which is the mapping of the Strategic Risks to the assurance activities to identify the potential gaps in the assurance over strategic risks. This should be used as a basis in developing the risk-based strategic internal audit plan and other assurance activities for the City.	Low	Prepare an assurance map of the Strategic Risks to identify potential gaps in assurance over strategic risks.	Governance & Strategy	Q4 FY 2024-2025

MOORE

Quick Search 🔍	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

Risk Management Process (cont.)

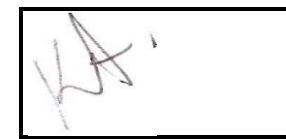|					
19.	Provide the contact details and **direct generic e-mail address** of the Risk Manager on the Risk Management intranet site for Council, Management, Staff, Contractors and Volunteers to have direct contact.	Low	Implement a risk email address such as Risk@cockburn.wa.gov.au and implement organisational training to educate staff on how it is to be used.	Governance & Strategy	Q4 FY 2024-2025
20.	• Timely review, approval and implementation of a comprehensive **Information and Cyber Security Policy** which is aligned to standards and better practice principles;	Medium	The administration *City of Cockburn Information and Cyber Security Policy* was approved by the CEO on 10 September 2019 and was due for review in September 2021. Conduct a review of the policy and incorporate amendments to implement a comprehensive Information and Cyber Security Policy which aligns to standards and better practice principles.	Finance	Q3 FY 2024-2025
	• Ensure that any Cyber Security Risk Assessment and gap analysis is presented to the ARC, with action plans being effectively tracked and monitored for closure; and		ICT Department to meet regular reporting to the ARC on Cyber Security Risk assessments and gap analysis, including monitoring of action plans.	Finance	Q3 FY 2024-2025
	• Maintain an IT Security Breach Register within the City.		ICT to develop and implement an IT security breach register.	Finance	Q3 FY 2024-2025
21.	**ICT Strategic Plan** – Timely review, approval and implementation of the Information Services Strategy Refresh which clearly outlines the ICT plans and projects to be executed, with timeline assigned for effective tracking and monitoring.	Medium	Review and implement the Information Services Strategy Refresh, with timeline assigned for effective tracking and monitoring.	Finance	Q3 FY 2024-2025

MOORE

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

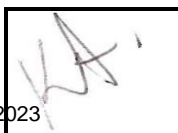| No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
22.	• **BCP and IM** - Ensure that the draft BCP is reviewed and revised to include other potential emergency events / incidents and align to the standards and better practice;		Complete a review of the BCP to include other potential emergency events/incidents and ensure it aligns to standards and better practice principles.	Governance & Strategy	
	• **CMP** - Timely review, approval and implementation of the Crisis Management Plan and Crisis Communication and align to the standards and better practice;		Review the City of Cockburn Crisis Management Plan and Crisis Communication Plan, and ensure timely reviews occur at least on a triennial basis.	Governance & Strategy/Corporate Affairs	Q3 FY 2023-2024
	• **EMP** - Timely review, approval and implementation of EMP. Provide testing or training to employee to create awareness;	High	Conduct a review the Emergency Management Plan and provide testing/training to employees, including implementation of a regular training program for employees.	Governance & Strategy/Community Services	Q3 FY 2023-2024
	• **DRP** - Timely review, approval and implementation of DRP and align to the standards and better practice; and		Review the *City of Cockburn Disaster Recovery Design Document*, and ensure timely reviews occur at least on a yearly basis.	Finance	Q3 FY 2023-2024
	• Perform BCM exercise and testing regularly and ensure that action plans arising from the exercise are effectively tracked and monitored for closure.		Perform BCM exercise and testing regularly. Adopt a process for management of actions from BCM exercises	Governance & Strategy	Q4 FY 2023-2024

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

| Quick Search | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

Risk Management Process (cont.)

23.	Maintain a **Privacy Breach Register** within the City.	Low	Develop and implement a Privacy Breach Register.	Governance & Strategy	Q3 FY 2024-2025
24.	• Develop and approve the **PID Policy and Procedures**, with version control date, approval details and City's branding; and	Medium	Develop PID Policy and Procedures.	Governance & Strategy	Q3 FY 2024-2025
	• Ensure that the PID officer contact in PSC PID Directory matched with the PID Officers in the City's website.		Review and ensure correct information is posted on the intranet.	Governance & Strategy	Q3 FY 2024-2025
25.	• Review and revise the Complaint Handling Procedures to ensure consistent and in line with the **Compliments, Feedback and Complaints Policy** and the Corporate Governance Framework;	Medium	Review the City of Cockburn Complaint Handling Procedures, to ensure consistent and in line with the Compliments, Feedback and Complaints Policy and the Corporate Governance Framework.	Governance & Strategy	Q3 FY 2024-2025
	• Only include accurate statements in the Compliments, Feedback and Complaints Policy after assessment done; and		Ensure to include only accurate statements in the Compliments, Feedback and Complaints Policy after assessment done.	Governance & Strategy	Q3 FY 2024-2025
	• Complaint Register: ○ Record the resolution dates in the Complaint Register for effective tracking and monitoring purposes; and		Ensure prompt recording of actions is completed in the Complaints Register.	Governance & Strategy	Q3 FY 2024-2025
	○ Include better practice metrics to efficiently and effectively manage the complaints and to monitor and report this to the ARC (e.g. trend on no. of complaints, types etc.).		Ensure to include better practice metrics to efficiently and effectively manage the complaints and to monitor and report this to the ARC.	Governance & Strategy	Q4 FY 2024-2025

MOORE

| Quick Search | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
26.	• Develop and / or revise and approve a comprehensive **FOI Policy** and Procedure which aligns to legislation, better practice principles and standards.	Low	Adopt a Freedom of Information policy	Governance & Strategy	Q4 FY 2024-2025
27.	• Review and revise the **WHS Policy**, with version control table to outline the adoption date and next review due; and	Medium	Review the WHS Policy to ensure it complies with the City's policy development guidelines and template.	People Experience & Transformation	Q2 FY 2023-2024
	• Develop and approve the WHS Procedures which aligns to legislation, better practice principles and standards.		Review the WHS Procedures to ensure compliance with the City's procedure development guidelines and template.	People Experience & Transformation	Q2 FY 2023-2024
28.	Develop and implement a **Register of Hazardous Materials**.	Low	Develop and implement a Register of Hazardous Materials.	People Experience & Transformation	Q4 FY 2023-2024
29.	Develop and approve a comprehensive **Fraud and Corruption Control Framework**, Fraud and Corruption Control Plan and Procedure, and, Fraud Incident Register which aligns to the legislation, better practice principles and standards. Organise fraud training to create awareness among staff.	Medium	Review the City's Fraud and Corruption Control Framework to align with legislation and better practice principles. Adopt a Fraud and Corruption Control Plan and Procedure, and Fraud Incident Register.	Governance & Strategy	Q3 FY 2024-2025

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

Quick Search	Executive Summary	Scope and Approach	Observations and Recommendations	Other	Appendices

Risk Management Process (cont.)

30.	Assess the achievement of **Risk Management Indicators** to measure performance of the Risk Management function and report to SLT, ARC and Council. Document the assessment as evidence. Ensure that current controls included under measurements in the RMF are implemented and in place. Otherwise, this may be seen as non-compliances.	High	Report on achievement of Risk Management Indicators to the SLT, ARC and Council.	Governance & Strategy	Q4 FY 2023-2024
31.	Timely review of **Risk Management Maturity Assessment** and ensure that key actions / recommendations arising from the review of the risk management framework are tracked and implemented.	Medium	Reporting and tracking of Risk Maturity Assessment actions to ARC annually.	Governance & Strategy	Q4 FY 2023-2024
32.	Include the recommendations for improvement in the future **CEO's Triennial Review** For Risk Management, Internal Control and Legislative Compliance.	Low	Review the CEO's triennial review for risk management, internal control and legislative compliance and implement the recommendations from the Risk Maturity Assessment.	Governance & Strategy	Q4 FY 2024-2025
33.	**Survey** a selection of Council Members, ARC Members, Risk Owners, Management, Staff, Contractors and / or Volunteers to identify continuous improvement opportunities and to gauge feedback on the current Risk Management Function and System.	Low	Identify opportunities for internal and external feedback for identification of continuous improvement opportunities.	Governance & Strategy	Q4 FY 2024-2025

MOORE

Page | 32

3.   OBSERVATIONS AND RECOMMENDATIONS (CONT.)

3.2   Key Observations (cont.)

Risk Management Process (cont.)

No	Recommendation	Risk Rating	Agreed Action	Responsible Owner	Action Date
34.	Consider the **use of data analytics** to analyse large volumes of data to identify current or emerging risks or opportunities within the City.	Low	Identify opportunities for use of data analytics to analyse data or identify current or emerging risks.	Governance & Strategy	Q4 FY 024-2025
35.	Consider the following **sources of better practice** and compare these to the City on a timely basis to identify improvement opportunities: • Auditor General tabled reports in all jurisdictions of Australia; • Risk Management Institute of Australasia; • Australian Institute of Company Directors; and • Governance Institute of Australia.	Low	Conduct regularly reviews against resources available from sources such as (but not limited to) the OAG, Risk Management Institute of Australia and Governance Institute of Australia to achieve continuous improvement.	Governance & Strategy	Ongoing

MOORE

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023

4. OTHER

4.1. Disclaimers

Moore Australia (WA) Pty Ltd as agent, an independent member of Moore Global Network Limited, and a Perth based partnership of trusts carries on business separately and independently from other Moore Global Network Limited member firms worldwide.

Services provided under this engagement are provided by Moore Australia (WA) Pty Ltd as agent and not by any other independent Moore Global Network Limited member firms worldwide. No other independent Moore Global Network Limited member has any liability for services provided.

4.2. Basis of Use

This report has been prepared in accordance with the objectives and approach agreed in the engagement document and subject to the following limitations:

- Other than use by you for the purpose, our report cannot be issued, accessed, or relied upon by any third party without our prior written approval. Furthermore, neither the report nor extracts from it will be included in any document to be circulated to other third parties without our prior written approval of the use, form, and context in which it is proposed to be released. We reserve the right to refuse to grant approval to issue the reporting to any other party;

- The matters raised in this report are only those which came to our attention while performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made. We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Accordingly, management should not rely on our report to identify all weaknesses that may exist in the systems and procedures under examination, or potential instances of non-compliance that may exist;

- We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy or reliability is given in relation to statements and representations made by, and the information and documentation provided by, Management and personnel. We have indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report. We are under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form unless specifically agreed with the client. The observations expressed in this report have been formed on the above basis; and

- Recommendations for improvement should be assessed by management for their full commercial impact, before they are implemented.

4.3. Conflicts of Interest

The firm is not aware of any existing or potential relationship, transaction or holding that would compromise its objectivity in the conduct of the services rendered. Should the possibility of a perceived or actual conflict arise the matter would be raised with the Chief Executive Officer immediately and activities suspended until the issue was resolved to your satisfaction.

4.4. Liability

Moore Australia (WA) Pty Ltd trading as agent – ABN 99 433 544 961, an independent member of Moore Global Network Limited - members in principal cities throughout the world.

Liability limited by a scheme approved under Professional Standards Legislation.

MOORE

| Quick Search 🔍 | Executive Summary | Scope and Approach | Observations and Recommendations | Other | Appendices |

APPENDIX 1: KEY TO SIGNIFICANCE OF RISK RATING

Rating	Definition	Guidance	Action required
High	Issue represents a control weakness, which could cause or is causing major disruption of the process or major adverse effect on the ability of the process to achieve its objectives.	• Material errors and departures from the organisation's policies and procedures; • Financial management / accountability / probity concerns. • Non-compliance with governing legislation and regulations may result in fines or other penalties; and • Collective impact of many moderate or low issues.	• Requires significant senior management intervention and may require significant mobilisation of resources, including external assistance; and • A detailed plan of action to be approved by Management with resolution within 30 days.
Medium	Issue represents a control weakness, which could cause or is causing moderate adverse effect on the ability of the process to meet its objectives.	• Events, operational, business, and financial risks could expose the organisation to losses could be marginally material to the organisation; and • Departures from best practice management procedures, processes.	• Requires substantial management intervention and may require possible external assistance; and • Timeframe for action is subject to competing priorities and cost benefit analysis but should not exceed 3 months.
Low	Issue represents a minor control weakness, with minimal but reportable impact on the ability to achieve process objectives.	• Events, operational and business risks could expose the organisation to losses which are not material due to the low probability of occurrence of the event and insignificant impact on the operating capacity, reputation, and regulatory compliance; and • Departures from management procedures, processes, however, appropriate monitoring and governance generally mitigates these risks.	• Requires management attention and possible use of external resources; and • Minor treatment is desirable. Action should be completed within 6 to 12 months.

MOORE

CONTACT US

Moore Australia (WA)

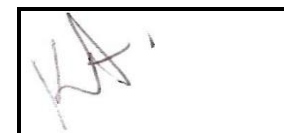Level 15, 2 The Esplanade,
Perth WA 6000

T　+61 8 9225 5355
F　+61 8 9225 6181
E　perth@moore-australia.com.au

www.moore-australia.com.au

MOORE

HELPING YOU THRIVE IN A CHANGING WORLD

11.4.2   (2023/MINUTE NO 0010) Audit Risk and Compliance Committee - Terms of Reference and Annual Calendar of Business

Responsible Executive	Executive Governance and Strategy
Author	Manager Legal and Compliance
Attachments	1. Audit Risk and Compliance Committee Terms of Reference ⇩
	2. Audit Risk and Compliance Committee Annual Calendar ⇩

Officer Recommendation/Committee Recommendation
MOVED Cr P Corke SECONDED Cr T Dewan

That Council:

(1)   ADOPTS the Audit Risk and Compliance Terms of Reference as attached to this Report.

<div align="right"><u>CARRIED 5/0</u></div>

Background

Council established the Audit Risk and Compliance Committee (ARC) on 10 March 2022.

The Council recommended the Terms of Reference be referred to the first ARC before adoption by Council.

The Terms of Reference were ultimately adopted by Council in April 2022.

The Terms of Reference have been subject to minor amendments over the last 12 months.

The purpose of this report is to present to the Committee, and Council recommended changes following an annual review.

Submission

N/A

Report

The review of the Terms of Reference has resulted in several recommended changes.

Consideration has also been given to recommendations from the Risk Maturity Review.

Key change themes include:

1. Addition of purpose: to clearly identify the purpose of the Committee;
2. Objectives and Duties – additions to a) "*which includes reviewing and ensuring the accuracy and completeness of the financial statements of the City of Cockburn*" and i) "*monitor and report on the effectiveness of the City's risk management framework, including reviewing risk assessments, risk treatment plans, and the effectiveness of controls*";
3. Membership – additions to add clarity to membership, no remuneration for independent members, training recommendations for ARC members to support ARC members in professional development and clarity around proxies and quorum requirements;
4. Meetings – not less than 4 per year with a commencement time of 6pm, removing the proposed end times as limitations should not be imposed or implied for the ARC;
5. Reporting – amendments to include current practices with agenda publications, and committee reporting duties to Council.

The Annual Calendar, which is indicative and an operational guide for ARC reporting, has been updated and is attached for the Committees reference.

Strategic Plans/Policy Implications

Listening & Leading
A community focused, sustainable, accountable and progressive organisation.
• Best practice Governance, partnerships and value for money.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

There are no budget implications from the recommendations in this report.

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

The recommended changes to the Terms of Reference address some of the issues identified in the Risk Maturity Review.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

Audit, Risk and Compliance Committee (ARC)

Terms of Reference

Purpose

The purpose of the ARC is to provide independent assurance and assistance to the Council in overseeing the financial reporting process, monitoring the effectiveness of internal control systems, assessing the management of financial and other risks, and ensuring compliance with relevant laws and regulations. The ARC also aims to promote transparency and accountability in the City's operations and to provide guidance and recommendations for continuous improvement of financial and risk management practices.

Background

1. The Audit, Risk and Compliance Committee (ARC) is a formally appointed Committee of Council.

2. The ARC does not have executive powers or authority to implement actions in areas over which the administration (management) has responsibility and remains independent of the administration.

Objectives and Duties

1. As part of the Council's obligations, Tthe ARC facilitates:

   a. external financial audit reporting which includes reviewing and ensuring the accuracy and completeness of the financial statements of the City of Cockburn;

   b. the examination of an Annual Financial Audit Report received and follow up of any matters raised in the rReport and subsequent management letter, to ensure appropriate action is taken in respect of those matters;

   c. vetting and responding to Office of the Auditor General (OAG) Local Government performance audits, whether the City is directly involved or not;

   d. compliance with the Council functions under Part 6 of the *Local Ggovernment aAct 1995* (the Act) in relation to the City's financial management;

   e. compliance with the Council functions under Part 7 of the Act in relation to Audit requirements;

   f. an appropriate internal audit program endorsed by Council;

   g. the review of the CEO's Report provided under:
      i. Regulation 17 (3) of the *Local Government (Audit) Rregulations 1996*; and
      ii. Regulation 5 (2) (c) of the *Local Government (Financial Management) Regulations 1996*;

   h. compliance with Regulation 17 of the *Local Government (Audit) Regulations 1996* in relation to:
      i. Risk management;
      ii. Internal control; and

        iii.   Legislative compliance;

and to review the appropriateness and effectiveness of the systems and procedures in relation to these matters on a triennial basis every three (3) financial years;

    i.   monitor and report on the effectiveness of the City's risk management framework, including reviewing risk assessments, risk treatment plans, and the effectiveness of controls;

    i.j.   effective communication between the external auditor, internal auditor, administration (management) and the Council;

    j.k.   effective management of financial and other risks to the City through a comprehensive risk management framework;

    k.l.   the protection of City assets; and

    l.m. review of the annual Compliance Audit Return required under Regulation 14 of the *Local government (Audit) Regulations 1996*.

2. The ARC performs any other function conferred on it by tThe Act, Regulations, or any other written law.

Membership

1. The Committee will comprise of a minimum of Elected Members four (4) Members, who shall be appointed by Council, and includes one (1) independent, appropriately qualified appointed member.

2. Payment of any fee to the independent member is prohibited by the Act.

3. No less than two proxies will be appointed, who will attend in the absence of a member.

1. A quorum shall be deemed present when at least half of the appointed Committee members are in attendance at a meeting.

4.

5. Elected Members who are ARC members (including proxies) will be encouraged to undertake training to support their role as ARC Members.

6. Training recommendations will be in accordance with the Executive Governance and Strategy recommendations.

2.7. The CEO and the officers responsible for the external and internal audit functions, risk management and legislative compliance will attend meetings to advise and provide information, as required and cannot be members.

3.8. Other City officers shall attend as required to provide administrative and secretarial support.

4.9. Representatives of the OAG and the contracted external and internal auditor shall be invited to attend the meetings as appropriate but must attend the meetings where the draft annual financial report and results of the external audit are to be considered.

Meetings
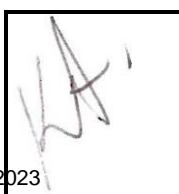
1.   The Committee shall meet on a quarterly basis or more frequently as required, with a minimum of four meetings per year~~the fourth Thursday in March, May, July, September, and November and on any other occasion necessitating the consideration of any function of the Committee.~~.

2.   The Committee shall be held in person at 6:00pm on meeting dates in accordance with Councils endorsed meeting schedule. ~~to 7:00pm or at 7:30 to 8:30pm on a rotating basis with the other 3 Committees as determined in advance in accordance with the two-year Electoral cycle.~~

3.2.   3.   An Audit Committee Calendar will be produced as guidance for the matters to be included on each regular meeting agenda and will be arranged to coincide with legislative timeframes where necessary

Delegation

1.   The ARC will be delegated the authority to meet with the appointed external auditor, as required by section 7.12A of t~~T~~he Act.
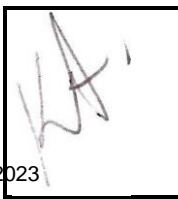
Reporting

1.   ~~The Committee shall ensure the preparation of meeting minutes to be forwarded to the next practicable ordinary Council Meeting for consideration by Council~~Agenda papers for the ARC will be published and made available to members no less than 7 days before a meeting.

1.2.   Reports and decisions of the ARC will be considered at the next Ordinary Council Meeting, or Special Council Meeting as may be required.

3.   The accompanying officer report will include all specific recommendations and a summary of the items considered at the relevant Committee meeting.

4.   The Committee shall report to Council any significant issues or concerns regarding financial management, internal control, risk management, or legislative compliance that it identifies during its activities.

Strategic Link:	
Category	Governance
Lead Business Unit:	Legal and Compliance
Public Consultation: **(Yes or No)**	No
Adoption Date: (Governance Purpose Only)	

Next Review Due: (Governance Purpose Only)	
ECM Doc Set ID: (Governance Purpose Only)	

Document Set ID: 11510391
Version: 4, Version Date: 22/08/2023
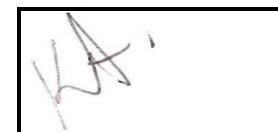
AUDIT, RISK AND COMPLIANCE (ARC) COMMITTEE

Terms of Reference – Objectives and Duties

1. External audit reporting on annual financial statements.

2. The examination of the annual financial audit report (Report) received and follow up of any matters raised in the Report and subsequent management letter, to ensure appropriate action is taken in respect of those matters.

3. Vetting and responding to Office of the Auditor General (OAG) Local Government performance audits, whether the City is directly involved or not.

4. Compliance with the Council functions under Part 6 of the *Local Government Act 1995* (the Act) in relation to the City`s financial management.

5. Compliance with the Council functions under Part 7 of the Act in relation to Audit requirements.

6. An appropriate internal audit program endorsed by Council.

7. The review of the CEO`s Report provided under:
   a. Regulation 17 (3) of the *Local Government (Audit) Regulations 1996*; and
   b. Regulation 5 (2) (c) of the *Local Government (Financial Management) Regulations 1996*.

8. Compliance with Regulation 17 of the *Local Government (Audit) Regulations 1996* in relation to:
   a. Risk management;
   b. Internal control; and
   c. Legislative compliance.

   and to review the appropriateness and effectiveness of the systems and procedures in relation to these matters on a triennial basis every three (3) financial years.

9. Effective communication between the external auditor, internal auditor, administration (management) and the Council.

10. Effective management of financial and other risks to the City through a comprehensive risk management framework.

11. The protection of City assets.

12. Review of the annual Compliance Audit Return required under Regulation 14 of the *Local Government (Audit) Regulations 1996)*.

AUDIT, RISK AND COMPLIANCE (ARC) COMMITTEE

Calendar of Business – 2 Year Election Cycle
Year 1

	September	November	March	May	July	September
Election 2021		Review of Monetary and Non-Monetary Investments	Compliance Audit Return (Part 7)	Review new FY Internal Audit Schedule	Audit Plan for End of Financial Year (OAG)	
		Annual Bad Debts Review and Write-offs		Review of systems and procedures for risk management; internal control; and legislative compliance (3 yearly program)	Audit Results Report – Annual Financial Audits of Local Government Entities (OAG)	
	Internal Audit Program Reporting	Annual Financial Audit Report		Strategic Risk Report	Risk Review Register	Internal Audit Program Reporting
	Operational Risk Report	Legal Proceedings between Council and Other Parties				

Standing Items
Audit Recommendations / Action Status Report
Review of OAG focus area/performance audits Report
Review of CCC Report
Legislative Changes
Notifiable incidents reporting
Notifiable compliance reporting

AUDIT, RISK AND COMPLIANCE (ARC) COMMITTEE

Calendar of Business – 2 Year Election Cycle
Year 2

November	March	May	July	September	
Review of Monetary and Non-Monetary Investments	Compliance Audit Return (Part 7)	Review new FY Internal Audit Schedule	Audit Plan for End of Financial Year (OAG)		Election 2023
Annual Bad Debts Review and Write-offs		Review of systems and procedures for risk management; internal control; and legislative compliance (3 yearly program)	Audit Results Report – Annual Financial Audits of Local Government Entities (OAG)		
Annual Financial Audit Report		Strategic Risk Report	Risk Review Register	Internal Audit Program Reporting	
Legal Proceedings between Council and Other Parties		Appointment of Independent Auditor			
Standing Items					
Audit Recommendations / Action Status Report					
Review of OAG focus area/performance audits Report					
Review of CCC Report					
Risk Management Reporting					
Notifiable incidents reporting					
Notifiable compliance reporting					

11.4.3   (2023/MINUTE NO 0011) Internal Audit Plan FY2024-2026

Responsible Executive	Executive Governance and Strategy
Author	Manager Legal and Compliance
Attachments	1. City of Cockburn Internal Audit Plan 2024-2026 Proposed ⇩

Officer Recommendation/Committee Recommendation

MOVED Cr T Dewan SECONDED Cr P Corke

That Council:

(1)   ADOPTS the proposed Internal Audit Plan FY2024-2026.

<u>**CARRIED 5/0**</u>

Background

The City of Cockburn's current Enterprise Risk Management Framework (RMF) subscribes to the four lines of defence assurance model promoted by the Office of the Auditor General (OAG), as the mechanism to provide assurance of effective risk management.

This model ensures roles, responsibilities and accountabilities for decision making are structured to demonstrate effective governance and assurance.

The four lines of assurance are as follows:

- First line - held by the Business/Service Unit Heads and employees
- Second line - held independently by the Legal and Compliance Service Unit
- Third line - provided by the City's internal/external auditing mechanism
- Fourth line - provided by the external performance and focus audits provided by the regulatory regimes – the Department of Local Government, Sport and Cultural Industries and the OAG.

As a third line of defence '*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes*' - definition from the *International Professional Practices Framework* issued by the Institute of Internal Auditors (IIA), 2017.

In October 2022 Council endorsed the Interim Internal Audit Plan for FY23, which comprised of an "Acting Through" audit.

The FY2024-2026 Internal Audit Plan is presented to the Audit Risk and Compliance Committee for endorsement by Council.

Submission

N/A

Report

The FY2024-2026 Internal Audit Plan comprises of several audits which were not delivered from the 2019-2022 Internal Audit Plan and a strategic risk identified in the City's risk register, which is categorised as an extreme risk.

As previously reported to the Audit Risk and Compliance Committee (ARC), when adopting the Interim Internal Audit Plan, several audits from the 2019-2022 Internal Audit Plan were not delivered due to the implications of COVID-19 in March 2020 and the resource limitations faced by the City at this time.

1. Contract Management

An evaluation of how the City manages contracts to verify and ensure that systems, policies, and controls (including resourcing capacity) are being met, and that all obligations and stipulations are taking place as agreed upon and scheduled.

2. Effectiveness of Service Delivery Planning and Review Processes

The audit objective is to assess the effectiveness of the City's service delivery planning and review processes, do they:

- Determine the viability and sustainability of the City's current service delivery model for services
- Forecast future demand and service needs
- Consider the best type of service delivery model (insource, outsource, mix etc.)
- Identify future funding challenges and solutions for controlling financial costs
- Survey and monitor community expectations (industry trends, benchmarking, customer satisfaction levels etc.)
- Measure the level and quality of services and require benefit analysis
- Consider and embrace technological changes
- Enable reshaping or repurposing of existing services.

To be undertaken in a staged approach with the first stage being a high-level review to determine overall current state and identify gaps and improvement opportunities.

Second (and future stages if necessary) will be to review specific areas identified and progress of improvement plan delivery).

3.   Fleet management

The objective of the audit is to assess the adequacy of the management control framework and related risk management strategies for the fleet management function, including processes relating to the planning, organizing, controlling, directing, communicating, and the management of vehicle assets. Extent to which the City's is complying with policies, procedures, guidelines, and with laws and regulations pertaining to fleet management.

4.   Climate Change Strategy – Adaptation

The City has identified key solutions in its climate resilience roadmap in the form of six adaptation objectives that will help the City increase resilience to climate change:
1.   Waterwise City
2.   Conserve biodiversity
3.   Coastal adaptation
4.   Increase the urban forest
5.   Protect community infrastructure
6.   Enhance health and wellbeing.

The audit objective is to assess the effectiveness of the six adaptation objectives that will help the City and its community increase resilience to climate change.

The first phase of this audit will be to create a program of work to schedule multiple audits, to track the implementation of the six mitigation objectives that will help the City mitigate climate change. This is due to the size and complexity of the 6 mitigation actions to achieve Net Zero by 2030.

The City will aim to deliver three internal audits each financial year.

Following the recent Risk Maturity Review undertaken by Moore Australia, subsequently reported on in this ARC meeting, there will be some additions to the Internal Audit Plan (FY2024-2026) to meet some of the recommendations.

Once this FY2024-2026 Internal Audit Plan is adopted, the City will commence the process to appoint an independent auditor.

Strategic Plans/Policy Implications

Environmental Responsibility
A leader in environmental management that enhances and sustainably manages our local natural areas and resources.
• Address Climate Change.

Listening & Leading
A community focused, sustainable, accountable and progressive organisation.
• Best practice Governance, partnerships and value for money.

Budget/Financial Implications

The City has an allocation for internal auditing services included in the annual budget each year.

Legal Implications

Local Government (Audit) Regulations 1996 Regulation 17.

Community Consultation

N/A

Risk Management Implications

The risk management implications of not having an internal audit plan are significant and could result in a number of negative consequences.

Without an internal audit plan, it is difficult to systematically identify, assess and manage risks that may impact the City of Cockburn.

Some potential risk management implications for not having an internal audit plan can include, increased risk of non-compliance, increased risk of operational inefficiencies and increased reputational risk.

It is recommended the incomplete audit items from the 2019-2022 Internal Audit Plan be included in the FY2024-2026 Internal Audit Plan to ensure they are completed and the relevant risks managed.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

139 of 146

City of Cockburn Internal Audit Plan 2024 – 2026 (Proposed) [ECM Doc Set ID: TBA]

Audit Name, Division, Owners	Reason	Likelihood	Consequence	Risk	Audit Scope	Organisational Context	2024	2025	2026
1. Contract Management Finance [ExCo member: Nelson Mauricio. Responsible Person: Tony Natale]	The potential costs and legal implications of contract noncompliance are so significant, it is vital to conduct regular audits to identify potential issues and opportunities within the existing contracts management processes. *Linked to Strategic Community Plan 2020–2030, Strategic Outcomes and Objectives; Listening and Leading - A community focused, sustainable, accountable, and progressive organisation* *Strategic Objectives - 5.1 Best practice Governance, partnerships, and value for money Measurements - Improved satisfaction with the City's Governance and financial sustainability.*	Possible 3	Minor 2	Moderate 6	An evaluation of how the City of Cockburn (the City) manages contracts to verify and ensure that systems, policies, and controls (including resourcing capacity) are being met, and that all obligations and stipulations are taking place as agreed upon and scheduled.	On 20 June 2022, the then Chief Financial Officer recommended scheduling this audit for the 2023 calendar year. The reason being that the Procurement Team were at capacity with tenders and the conversion from *Ci* to *Ci – Anywhere* until December 2022.	✔		
2. Effectiveness of Service Delivery Planning and Review Processes Governance and Strategy [ExCo member: Emma Milne. Responsible Person: Jane Downsborough]	Over time, the needs and expectations of communities can change. The City should have robust and comprehensive processes for service planning and review to ensure all services continue to provide value for money that is in line with community expectations. Community engagement is a critical aspect in prioritising resources for service provision against other responsibilities such as asset maintenance and capital works. How does the City ensure it remains focused on the delivery of services at optimal service levels that match community expectations and use the best, most efficient delivery models? *Extracted from the City of Cockburn Strategic Community Plan 2020-2030:* *Community, Lifestyle and Security objective 3.1 –* *'Provide a diverse range of accessible, inclusive and targeted community services, recreation programs, events and cultural activities that enrich our community.'* *City Growth and Moving Around objective 4.2 –* *'Sustainable revitalise urban areas to deliver high levels of amenity and to cater for population growth.'*	Unlikely 2	Critical 4	Moderate 8	The audit objective is to assess the effectiveness of the City's service delivery planning and review processes, do they: • Determine the viability and sustainability of the City's current service delivery model for services, • Forecast future demand and service needs. • Consider the best type of service delivery model (insource, outsource, mix etc.), • Identify future funding challenges and solutions for controlling financial costs, • Survey and monitor community expectations (industry trends, benchmarking, customer satisfaction levels etc.), • Measure the level and quality of services and require benefit analysis. • Consider and embrace technological changes, • Enable reshaping or repurposing of existing services. To be undertaken in a staged approach with the first stage being a high-level review to determine overall current state and identify gaps and improvement opportunities. Second (and future stages if necessary) will be to review specific areas identified and progress of improvement plan delivery).	On 02 June 2020, the then Executive Manager Strategy & Civic Support recommended that this audit be postponed after the COVID-19 pandemic restrictions were removed because this audit required significant input and resources from all business and service units in the organisation. On 04 November 2022, the Manager Strategy, and Integrated Planning stated that assessing the effectiveness of the services required meaningful KPIs and determining indicators for service level. This information should be included in the service plans.		✔	

City of Cockburn Internal Audit Plan 2024 – 2026 (Proposed) [ECM Doc Set ID: TBA]

Audit Name, Division, Owners	Reason	LikelihLood	Consequence	Risk	Audit Scope	Organisational Context	2024	2025	2026
3. Fleet Management Operations [ExCo member: Anton Lees. Responsible Person: Lou Viera]	The City has a considerable investment in its fleet assets and considerable resources are consumed in operating and maintaining the fleet to ensure it services the City's business requirements. Independent review will assist the City to determine the effectiveness of the fleet management model. *Linked to Strategic Community Plan 2020–2030, Strategic Outcomes and Objectives; Listening and Leading - A community focused, sustainable, accountable, and progressive organisation* *Strategic Objectives - 5.1 Best practice Governance, partnerships, and value for money Measurements - Improved satisfaction with the City's Governance and financial sustainability.*	Unlikely 2	Major 3	Moderate 6	The objective of the review is to assess the adequacy of the management control framework and related risk management strategies for the fleet management function, including processes relating to the planning, organizing, controlling, directing, communicating, and the management of vehicle assets. Extent to which the City's is complying with policies, procedures, guidelines, and with laws and regulations pertaining to fleet management.	Emerging Strategic and Operational Risks		✔	
4. Climate Change Strategy - Adaptation Built and Natural Environment [ExCo member: Daniel Arndt. Responsible Person: Christopher Beaton]	Climate change has significant social, economic, and legal implications for local government. The City is already experiencing effects with increased coastal erosion, higher summer temperatures, more severe heatwaves and a longer bushfire season. The City has a critical role in responding to climate change through its responsibilities for land use planning, emergency management, ownership of public infrastructure and delivery of community services. On 22 April 2020 Ernst and Young facilitated a risk assessment for the City, to update its climate change risk register. The process considered the consequences and likelihood of 18 climate risks using the City's ratings frameworks, which are consistent with AS ISO 31000:2018 *Risk management Guidelines*. The 18 risks have been grouped into their areas of impact and consolidated into the six overarching risks below: 1. Reduced water availability from decreased rainfall 2. Biodiversity loss from sea level rise 3. Coastal impacts from sea level rise 4. Urban forest decline from climate change 5. Community infrastructure damage from climate change impacts. 6. Public health decline from climate change	Likely 4	Catastrophic 5	Extreme 20	The City has identified key solutions in its climate resilience roadmap in the form of six adaptation objectives that will help the City increase resilience to climate change: 1. Waterwise City 2. Conserve biodiversity 3. Coastal adaptation 4. Increase the urban forest 5. Protect community infrastructure 6. Enhance health and wellbeing The audit objective is to assess the effectiveness of the six adaptation objectives that will help the City and its community increase resilience to climate change. The first phase of this audit will be to create a program of work to schedule multiple audits, to track the implementation of the six mitigation objectives that will help the City mitigate climate change. This is due to the size and complexity of the 6 mitigation actions to achieve Net Zero by 2030.	The vision of the *City of Cockburn Climate Change Strategy 2020-2023* is for the City to continue to be a leader in climate resilience and sustainability. The City aspires to become a carbon neutral City and commit to working with the community to adapt to our changing climate.		✔	✔

Page 2 of 2

11.5 People Experience and Transformation

11.5.1 (2023/MINUTE NO 0012) Organisational Culture Review by Independent Member - Quotation

Responsible Executive	Acting Executive, People Experience and Transformation
Author	Acting Executive, People Experience and Transformation
Attachments	1. Proposal One - Mapien **(Confidential)** 2. Proposal Two - Keogh **(Confidential)** 3. Proposal Three - Integral Development Associates **(Confidential)**

Officer Recommendation/Committee Recommendation

MOVED Cr T Dewan SECONDED Cr P Corke

That Council:

(1) RECEIVES the proposals received and attached to the report; and

(2) DEFERS consideration of the Organisational Culture Review to an Audit Risk and Compliance Meeting to be held within six months of the commencement of the Chief Executive Officer.

CARRIED 5/0

Background

The following Council Decision was made at the 13 October 2022 Ordinary Council Meeting, Council

That Council:

(1) RECEIVES the Minutes of the 21 September 2022 Audit, Risk and Compliance Committee Meeting.

(2) ADOPTS the recommendations contained within.

(3) REQUESTS quotations for Council consideration for an external review of the City's policies covering workplace bullying and harassment, and workplace bullying, and harassment claims made in 2022; and

(4) REQUESTS quotations for Council consideration of an Organisational Culture Review by an independent consultant.

Submission

N/A

Report

Organisational Culture Review

The City has requested quotations in relation to the undertaking of an organisational cultural review by an independent consultant.

The following scope was provided to prospective consultants:

- Analysis of previous engagement surveys, pulse surveys, exit surveys and other People Experience metrics to ascertain the status of the organisational culture at the City.
- The review must include
  o Direct, in person engagement of employees, including interviews and focus groups.
  o A whole of business engagement survey.
- Debrief to be undertaken with the Chief Executive Officer, Executive Committee (ExCo) and Council.
- Recommendations made in relation to short comings and areas of improvement in relation to organisational culture at the City.

A recent pulse survey, coordinated in December 2022, indicated three main areas of concern:

1. A lack of capability and trust with senior leaders.
2. The unresolved Enterprise Agreement process.
3. The uncertainty involved in the Chief Executive Officer recruitment process.

Of these areas of concern two are deemed to be resolved, with a comprehensive strategy relating to leadership capability in development. An organisational wide engagement survey is scheduled to take place in late May 2023.

It is proposed that any decision pertaining to the commencement of an organisational culture review is deferred to an ARC Meeting that is held within six months of the commencement of the Chief Executive Officer.

Review of City Policy - Bullying and Harassment

The City's current Bullying, Harassment and Discrimination Policy is an Administration Policy.

It was reviewed and endorsed by the Executive Committee on 24 February 2023.

The Policy was drafted in line with best practice processes and compliant to relevant legislation.

The Policy was peer reviewed by WALGA prior to endorsement.

<u>Workplace Bullying and Harassment Claims</u>

Any claims made by employees in relation to bullying and harassment are a confidential employee matter and will not be disclosed.

Strategic Plans/Policy Implications

<u>Listening & Leading</u>
A community focused, sustainable, accountable, and progressive organisation.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

The costs associated with undertaking an independent organisational culture review has not been budgeted for in FY23 or FY24.

If the Council were to proceed with an independent organisational culture review a budget provision will be required.

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

Poor organisational culture can have implications on attraction and retention of employees, as well as having an impact on the overall strategic and operational performance of the organisation.

The City currently undertakes regular engagement activities with whole of business to ensure that feedback is captured, and strategies are developed and implemented promptly with the aim of improving employee engagement.

Should an independent organisational culture review take place prior to the commencement of the Chief Executive Officer, there will be no ability for the incumbent to actively participate in this process.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

145 of 146

12. Motions of Which Previous Notice Has Been Given

Nil

13. Notices Of Motion Given At The Meeting For Consideration At Next Meeting

Nil

14. New Business of an Urgent Nature Introduced by Members or Officers

Nil

15. Matters to be Noted for Investigation, Without Debate

Nil

16. Confidential Business

Nil

17. Closure of Meeting

There being no further business, the Presiding Member closed the meeting at 6.23pm.