Shire of Coolgardie
Mother of the Goldfields

AGENDA

Audit Committee Meeting

16 July 2024

4:30pm

Kambalda Recreation Centre, Barnes Drive, Kambalda

SHIRE OF COOLGARDIE

NOTICE OF AUDIT COMMITTEE MEETING

Dear Elected Member

The next Audit Committee Meeting of the Shire of Coolgardie will be held on Tuesday 16 July 2024 commencing at 4:30pm.

REBECCA HORAN
ACTING CHIEF EXECUTIVE OFFICER

DISCLAIMER

INFORMATION FOR PUBLIC ATTENDING COUNCIL MEETINGS

PLEASE NOTE:

THE RECOMMENDATIONS CONTAINED IN THIS AGENDA ARE OFFICERS RECOMMENDATIONS ONLY AND SHOULD NOT BE ACTED UPON UNTIL COUNCIL HAS RESOLVED TO ADOPT THOSE RECOMMENDATIONS.

THE RESOLUTIONS OF COUNCIL SHOULD BE CONFIRMED BY PERUSING THE MINUTES OF THE COUNCIL MEETING AT WHICH THESE RECOMMENDATIONS WERE CONSIDERED.

MEMBERS OF THE PUBLIC SHOULD ALSO NOTE THAT THEY ACT AT THEIR OWN RISK IF THEY ENACT ANY RESOLUTION PRIOR TO RECEIVING OFFICIAL WRITTEN NOTIFICATION OF COUNCILS DECISION.

Rebecca Horan
ACTING CHIEF EXECUTIVE OFFICER

Order Of Business

1 DECLARATION OF OPENING / ANNOUNCEMENT OF VISITORS

2 RECORD OF ATTENDANCE / APOLOGIES / APPROVED LEAVE OF ABSENCE

3 DECLARATIONS OF INTEREST

3.1 Declarations of Financial Interests – Local Government Act Section 5.60A

3.2 Declarations of Proximity Interests – Local Government Act Section 5.60B

3.3 Declarations of Impartiality Interests – Shire of Coolgardie Code of Conduct for Council Members, Committee Members and Candidates for Election, Code of Conduct for Employees

4 CONFIRMATION OF MINUTES OF PREVIOUS MEETINGS

4.1 MINUTES OF THE AUDIT COMMITTEE MEETING HELD ON 5 MARCH 2024

Date: **9 July 2024**

Author: **Kasey Turner, Executive Assistant**

ATTACHMENTS

Nil

VOTING REQUIREMENT

Simple Majority

OFFICER RECOMMENDATION

That the Minutes of the Audit Committee Meeting held on 5 March 2024 be confirmed as a true and accurate record.

5 REPORTS OF OFFICERS

5.1 Executive Services

5.1.1 OFFICE OF AUDITOR GENERAL (OAG) - REPORT - LOCAL GOVERNMENT DISASTER RECOVER PLANNING

Location: Shire of Coolgardie

Applicant: Nil

Disclosure of Interest: Nil

Date: 2nd July 2024

Author: Steven Tweedie, Consultant

SUMMARY

That the Audit Committee note the advice provided by the CEO in relation to the recent OAG Report – Local Government IT Disaster Recovery Planning.

BACKGROUND

The Office of the Auditor General (OAG) has recently tabled a Report – Local Government IT Disaster Recovery Planning.

https://audit.wa.gov.au/wp-content/uploads/2024/05/Report-17_Local-Government-ICT-Disaster-Recovery-Planning.pdf

COMMENT

This audit assessed whether six non-metropolitan local government entities of varying sizes effectively plan and test their ability to recover their information technology systems following a disaster.

An assessment of how the Shire of Coolgardie compares with the issues and recommendations is attached and a further report will be provided to a subsequent Audit Committee, if updates are needed.

The OAG states:

"My Office's previous information systems audits have consistently found issues with local government disaster recovery planning.

This audit was an opportunity to delve a little deeper into entities' preparedness. Encouragingly, all the entities we audited were aware of the importance of disaster recovery planning to recover their IT systems and most had developed plans.

However, none were fully prepared. Further, as all the entities we audited relied on third party vendors to manage and recover their IT systems, it is important that vendor service agreements clearly define what is to be delivered.

I encourage entities to use the better practice principles we have included in this report to improve disaster recovery planning across the local government sector.

Timely recovery of IT systems after a disaster can reduce financial and reputational losses, and minimise delays in delivering services to the public."

Findings included:

- Entities did not appropriately document how they plan to recover their IT systems
  - Most entities did not fully document how they will respond to a disaster.
- Entities did not know if their plans would work as expected
- Service agreements with IT vendors were not adequate
  - Entities' agreements with IT vendors were not detailed enough to deal with disasters. All the entities relied on IT vendors to participate in disaster recovery planning and testing and to respond in case of disasters

The Report concludes –

"**None of the audited entities were ready to recover their IT systems following a disaster as they had not effectively planned or tested their DRPs (Disaster recovery Plan). All acknowledged the importance of disaster recovery planning and most had developed DRPs.**

However, only one DRP was adequate and none had tested if their plans would work.

Appropriate planning and testing help reduce the likelihood of prolonged system outages that can disrupt business operations, the delivery of services to the community, and be costly to fix.

All the audited entities used third party vendors to manage and recover their IT systems.

However, none had adequate service agreements in place. The agreements did not clearly define entities' recovery expectations or vendors' obligations to prepare and test plans.

In one case, the entity did not have a formal arrangement in place and relied on a verbal understanding.

Clear and appropriate service agreements help ensure vendors understand an entity's needs and will prepare for and respond to a disaster as expected."

OAG Report Recommendations – relating to 6 non metro LGs assessed	SoC level of compliance or readiness	SoC actions underway, or to be taken
1. assess their recovery requirements and appropriately document detailed disaster recovery plans. Consideration should be given to key elements as outlined in Appendix 1 of report - below **Better practice principles – key elements of IT disaster recovery plans**		
<u>Purpose and scope</u> The purpose and scope of the plan should be defined and agreed with senior management. It should include: • details and location of the main technology supporting the business • an overview of the organisation and people that manage the technology • the security classification of systems • the relationship of this plan to other business continuity, incident response and cyber security response plans.	**The plan describes how the Shire of Coolgardie will respond to a range of scenarios that may impact the organisation. It describes the roles required, who will fill them and the priorities that the response team should observe in the event of a disaster scenario.** **The plan contains locations and technology supporting the organisation.**	**Further improvement can be made by providing detail of the organisation maintaining and responsible for IT during a DR event and the security and classification of the system. Cyber response plans should be considered within the DR plan, including more detailed descriptions of incident response plans and their relevance to the DR plan.**
<u>Roles and responsibilities</u>	**Coolgardie's current Disaster Recovery Plan highlights**	**The Disaster Recovery Plan needs updated delegated**

Cleary define the positions, teams and IT vendors with responsibilities for governance, incident escalation and IT disaster recovery. These should have the appropriate skills and knowledge, or contractual arrangements in place. Decision-making and spending authorities should also be clearly documented.	**positions, IT Vendors, teams and responsibilities for each position throughout the DR process.**	**positions and the details of each person and their responsibilities to update the documentation.**
Contact details Contact details for all key external and internal stakeholders.	**Market Creations (Integrated ICT) 9920 8555 or servicedesk@integratedict.com.au**	**Update specific key internal stakeholders contact details and add in specific key external stakeholder contact details.**
Plan activation Clearly document the circumstances and timeframes that cause the plan to be invoked.	**The disaster recovery incident manager notifies other members of the recovery team and IT recovery team to inform them of the disaster and extent of damage in the areas of responsibility.** **The most appropriate recovery strategy is agreed, and the IT recovery team commence activities as described in the chosen strategy. A disaster is defined as being a situation such that access to Synergy is unlikely to be achieved within 2 days without resorting to the DR plan.**	**Additional consideration to shire services should be undertaken to establish areas of criticality which may affect organisation continuity. Services identified should then be considered for enactment of DR based on timeframe of restoration.**
Recovery objectives Entities should assess the risks and effects a disaster will have to key IT systems. Plans should reflect the current business needs of the entity and outline: • critical business functions and their supporting IT systems. These should be listed in order of importance • recovery time objectives (RTO) - the timeframes in which the IT systems are to be recovered • recovery point objectives (RPO) - the amount of data which can be lost, measured in time.	**While the plan acknowledges the roles, locations and events of disaster, No RTO's or RPO's are clearly defined.**	**Clearly develop Recovery Time and Point Objectives and update the Disaster Recovery Plan accordingly. Update the Disaster Recovery Plan to be suitable with the current environment in which it is being deployed to.**
Recovery procedures A description of, or direction to, recovery procedures for: • networks, servers, applications and databases • security systems • data synchronisation within and between applications, including potential procedures to handle a backlog of information	**A description and direction of recovery procedures are present for Networks, servers, applications and databases. A description/direction of Security Systems is not mentioned. There is no specific recovery procedures are mentioned for data synchronisation and data restoration, there is a recovery**	**Develop specific procedures addressing each key recommendation highlighted by the OAG.**

• data restoration • handover of services to users.	**procedure and direction of data restoration.**	
Communication plan Plans should outline the method and frequency of communication to key stakeholders such as the public, enforcement authorities and other government departments.	**Once damage to IT equipment and related facilities has been assessed, the disaster recovery incident manager must notify relevant authorities to establish priorities and cooperation with government and other supporting organisations.**	**The DR plan should be revised to include regular communication frequency guidelines and provide a clearer list of stakeholders.**
Document control and storage Plans should include clear approvals, version control and where the plan will be stored.	**While version control mechanisms are in place, there has been no version control for the roll out of the Disaster Recovery Plan or documentation since its inception. The plan includes clear approvers in Joel Newey and Bec Horan, however these need updating.**	**Review Version Control management and update approvals and clear lines of responsibilities.**
Testing Plans need to be tested to ensure they can recover IT systems and will work as expected. They should detail the intended frequency, nature and scope of testing.	**One test was conducted successfully in 2021 following this plan. Testing was not completed in 2022 or 2023. The plan highlighted that testing should be conducted annually to follow best practice and clearly highlights Scope and Nature of the test.**	**Formulate dedicated testing routines and review testing scope.**
2. periodically test their recovery plans, to verify that key IT systems and information can be restored in line with entity expectations		
3. review and update their IT vendor service agreements to include obligations for disaster recovery planning, testing and response. Any recourse if services are not met should also be documented.		

CONSULTATION

Bec Horan, Director Governance and Administration

Integrated ICT, Shire's IT Consultants

STATUTORY ENVIRONMENT

Nil

POLICY IMPLICATIONS

It is possible that an outcome of the assessment of the issues in the report may lead to changes to some internal policies and procedures.

FINANCIAL IMPLICATIONS

IT Related expenses are accounted for within the 2024/2025 budget.

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

Nil

VOTING REQUIREMENT

Simple Majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That

1. **The Audit Committee note the advice provided by the CEO in relation to the recent OAG Report – Local Government IT Disaster Recovery Planning.**
2. **That the CEO provide a further report to the Audit Committee and Council regarding action taken to address and implement recommendations relevant to the Shire administration which have not been addressed as at the date of this report.**

5.1.2 OFFICE OF AUDITOR GENERAL (OAG) - LOCAL GOVERNMENT 2022-2023 FINANCIAL AUDIT RESULTS

Location: **Shire of Coolgardie**

Applicant: **Nil**

Disclosure of Interest: **Nil**

Date: **2nd July 2024**

Author: **Steven Tweedie, Consultant**

SUMMARY

That the Audit Committee is pleased, that with one small exception, the Shire of Coolgardie has received no adverse findings or reports from the OAG, as revealed in Local Government 2022-23 – Financial Audit Results.

BACKGROUND

The Office of the Auditor General (OAG) has recently tabled in State Parliament its report - **Local Government 2022-23 – Financial Audit Results:**

https://audit.wa.gov.au/wp-content/uploads/2024/06/Report-18_Local-Government-2022-23-Financial-Audit-Results.pdf

COMMENT

The recently tabled report of the Office of the Auditor General (OAG) - **LOCAL GOVERNMENT 2022-23 – FINANCIAL AUDIT RESULTS** has relevance to the Shire of Coolgardie. The Report also relates to another recently tabled OAG Report - **Local Government 2022-23 – Information Systems Audit Results** – see separate agenda item.

The Auditor General states in her Report:

"As I reflect on the 2022-23 audit season – our second year auditing the entire local government sector – we are starting to see the impact of the hard work put in by the sector and our stricter timing initiative.

Previously, we have provided greater assistance to entities but at financial cost and later publication of financial reports. This year nearly 90% of audit opinions were signed by 31 December 2023 (compared to just 61% by the same time last year), without any significant change in audit outcomes.

We are now in a better place to get a holistic and truer picture of the sector earlier than we did last year.

Pleasingly, we have seen an overall reduction in the number and significance of financial management control issues reported to entities.

However, financial reporting, asset and procurement issues remain at relatively high levels. In addition, completeness and accuracy of asset registers and valuations continue to cause significant difficulties for entities.

In particular, valuations are too often accepted without review or question by entity management.

We see huge movements in values that entities often cannot explain, suggesting that they have not engaged in any meaningful way with the valuation process and the judgements made for accounting purposes.

This increases the risk of errors and generally requires additional audit work and cost. Significant changes in asset values should be adequately explained and supported by logic and evidence.

Entities continue to request more guidance with the valuation process. The Department of Local Government, Sport and Cultural Industries (DLGSC) is undertaking a body of work to prepare a valuation guide for the sector.

We are hoping the guide will help entities address the issues we continue to see around valuations, including seeking valuations that appropriately recognise restrictions on land use.

Unfortunately, information systems control issues continue to grow and remain unresolved from previous years. A full analysis of these results is contained within my Local Government 2022-23 – Information Systems Audit Results report.

Entities can improve the cost and timeliness of their audits by focussing on fixing issues, particularly those from prior years. Issues which continue year after year present a real financial management risk to entities.

Assessing and following up on these issues also requires extra audit work, resulting in increased costs to entities."

To further improve financial reporting timeliness and reduce costs OAG recommends entities should:
a. submit good quality, reviewed and CEO-signed financial reports for audit no later than 30 September. Supporting work papers and reconciliations should also be available by this date
b. communicate delays to financial report submission early to minimise disruptions and facilitate resource allocation. Flexibility may be required from entities when rescheduling their audit
c. engage early with valuers to develop a scope and plan for valuation. This is essential to ensure timely, compliant and sensible valuations. Entity information provided to valuers should be complete and accurate
d. alert OAG audit engagement leaders to new processes or systems, any issues encountered during the year, or any area of concern or technical accounting determinations
e. evaluate the significance of errors and decide if they need to be adjusted. Analyse the root cause for the errors.

The Report indicates that there was/were:

- 1 disclaimed opinion – did not include SoC
- 9 qualified opinions – did not include SoC

OAG has commented on the "status and timeliness of audits", and in relation to SoC, the latter received:

- Type of opinion report - Clear opinion with emphasis of matter or matter of significance paragraph
    - Restatement of Comparative balances We draw attention to Note 30 of the financial statements which states that the amounts reported in the previously issued 30 June 2022 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
        - ✓ Two prior period errors were corrected. One correction related to an error in the 2018 valuation of unsealed road infrastructure and the other related to incorrect accounting for a revaluation decrement for other infrastructure.
- Financial report timeliness – audit ready submissions - Extension or statutory deadline was not met with audit ready financial report.

SoC:

- is NOT listed as an entity who received an extension from DLGSC to submit their financial report after the 30 September legislated deadline,
- did NOT receive a qualified opinion,
- did NOT need any prior year qualifications removed.

CONSULTATION

Nil

STATUTORY ENVIRONMENT

Nil

POLICY IMPLICATIONS

Nil

FINANCIAL IMPLICATIONS

Nil

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

Nil

VOTING REQUIREMENT

Simple Majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That the Audit Committee is pleased, that with one small exception, the Shire of Coolgardie has received no adverse findings or reports from the OAG, as revealed in Local Government 2022-2023 – Financial Audit Results.

5.1.3 LOCAL GOVERNMENT INQUIRY

Location: NIL

Applicant: NIL

Disclosure of Interest: NIL

Date: 3rd July 2024

Author: Rebecca Horan, Director of Governance and Administration

SUMMARY

That the Audit Committee recommends to Council, that Council notes the final report outlining the Inquiry Recommendation and actions, endorses the implementation and completion of the Inquiry recommendations and requests the CEO provides the Audit Committee and Ordinary Council Meeting minutes to the Department of Local Government, Sport and Cultural Industries

BACKGROUND

Council at its Ordinary Meeting of Council held on the 19th December 2023 resolved the following:-

COUNCIL RESOLUTION #1/2023

Moved: Cr Kathie Lindup
Seconded: Cr Tracey Rathbone

That Council:

1. **Receive the Report of the Inquiry into the Shire Coolgardie.**
2. **Authorise the Chief Executive Officer in accordance with the provisions of Section 8.14(3) of the Local Government Act 1995, to provide the Minister with written advice setting out the things that the Shire has done or proposes to do to give effect to the recommendations contained in the report by 4th January 2024 – noting that the CEO, in conjunction with Council has already undertaken the process to secure relevant training for Council Members, and staff in January 2024pertaining to conflict of interest training for Council, and staff, in relation to Recommendation 1 of the Inquiry Report.**
3. **Authorise the Chief Executive Officer to seek legal advice on any potential implications from the recommendations and conclusions in the Report of the Inquiry into the Shire Coolgardie.**

In Favour: **Crs Malcolm Cullen, Tracey Rathbone, Sherryl Botting, Kathie Lindup, Rose Mitchell, Daphne Simmons and Corey Matthews**

Against: **Nil**

CARRIED 7/0

COMMENT

Staff have engaged the services of consultants to work through the recommendations from the Inquiry.

Hammond and Woodhouse were engaged to conduct Conflict of Interest Training for Council members and the management group and Chris Liversage from Conway Highbury as conducted the review of the Shire's procurement/purchasing policy and procedures.

The review and update of the professional development and training program for council members and staff has been conducted internally.

The Shire received confirmation from the Department via email on Wednesday 3rd July 2024 that they have reviewed all of the documents provided and are of the view that all three recommendations have now been completed.

CONSULTATION

Chris Liversage, Conway Highbury

Andrew Hammond and John Woodhouse, Hammond and Woodhouse Advisory

Department of Local Government

STATUTORY ENVIRONMENT

N/A

POLICY IMPLICATIONS

N/A

FINANCIAL IMPLICATIONS

N/A

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

1. Recommendations and Actions - Final

VOTING REQUIREMENT

Simple Majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That the Audit Committee recommends to Council, that Council

1. **NOTES the final report outlining the Inquiry Recommendations and actions implemented as outlined in the attachment.**
2. **ENDORSES the implementation and completion of the Shire of Coolgardie Inquiry Recommendations; and**
3. **REQUESTS the CEO provides the Audit Committee and Ordinary Council Meeting minutes to the Department of Local Government, Sport and Cultural Industries evidencing Council's endorsement of the implementation of the Inquiry Recommendations.**

5.1.4 RISK AREA SUMMARY

Location: **All areas**

Applicant: **Nil**

Disclosure of Interest: **Nil**

Date: **9 July 2024**

Author: **Rebecca Horan, Director of Governance and Administration**

SUMMARY

That the Audit committee receive the risk area summary reports as attached.

BACKGROUND

Management staff are monitoring their risks through the PULSE (Shires Risk Reporting System). Staff will report to the Audit committee quarterly or as requested.

COMMENT

All risks have been entered into the PULSE system and those risk owners are to action them accordingly.

CONSULTATION

Management Staff

STATUTORY ENVIRONMENT

Local Government (Audit) Regulation 17

POLICY IMPLICATIONS

Policy Number 2.12 Occupational Safety and Health

Policy 2.6 Risk Management

FINANCIAL IMPLICATIONS

Nil

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

1. Risk Area Summary Report - July 2024 - Confidential

VOTING REQUIREMENT

Simple majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That Audit Committee RECEIVE the Risk Area Summary reports as attached.

5.1.5 OFFICE OF AUDITOR GENERAL (OAG) - LOCAL GOVERNMENT 2022-2023 INFORMATION SYSTEMS AUDIT RESULTS

Location: **Shire of Coolgardie**

Applicant: **NIL**

Disclosure of Interest: **NIL**

Date: **9th July 2024**

Author: **Steven Tweedie, Consultant**

SUMMARY

That the CEO give effect to implementing, where necessary, in a timing and cost-effective manner, the findings and recommendations of the OAG Report - Local Government 2022-23 – Information Systems Audit Results, and where appropriate, report back to Council, via the Audit Committee on issues and implications.

BACKGROUND

The Office of the Auditor General (OAG) has recently tabled in State Parliament its report - **Local Government 2022-23 – Information Systems Audit Results:**

https://audit.wa.gov.au/wp-content/uploads/2024/05/Report-16-_Local-Government-2022-23-Information-Systems-Audit-Results.pdf

COMMENT

The recently tabled report of the Office of the Auditor General (OAG) - Local Government 2022-23 – Information Systems Audit Results has relevance to the Shire of Coolgardie.

The Auditor General states in her Report:

"Our audit results show entities have improved the maturity of their control capability since our first information system audits in 2019-20, with the biggest improvements in risk and change management.

However, significant improvements are still needed in all other areas.

Information and cyber security remains the highest concern due to the number of weaknesses we continue to identify in the five related categories (access management, endpoint security, human resource security, network security and information security framework).

Entities need to better protect themselves against external and internal threats to reduce the risk of security breaches. Internal threats can be notably reduced through fit for-purpose human resource controls such as screening, onboarding and offboarding procedures, and cyber security education programs.

This year, we reported 473 (58 significant, 328 moderate, 87 minor) issues to 76 entities.

Concerningly, a large proportion (45%) of significant issues were unresolved findings from last year."

OAG encourages LGs to implement the Australian Cyber Security Centre's mitigation strategies designed to protect against common cyber threats with a key focus on Essential Eight controls:

- Access management - common weaknesses included:

  - **Administrator privileges were not well managed – excessive numbers of individuals were given administrator privileges. Administrators did not have separate nonprivileged accounts for day-to-day tasks and administrator activity was not logged and monitored. Highly privileged accounts must be well managed as they can change system configurations, access rights and data.**
  - **Access and activity were not logged and monitored – application, database and network access and activity were not appropriately logged or monitored to detect malicious activity. Entities should use fit-for-purpose tools to correlate and monitor activity from different systems (e.g. network, applications and databases).**
  - **Multi-factor authentication (MFA) was not used or not applied to all accounts – a lack of MFA can increase the likelihood of unauthorised access.**
  - **Access was not reviewed – entities did not review accounts to ensure they are required and have least privileges assigned to perform their function. Without a review of accounts (application, network, database, remote access, generic, system and administrator) there is an increased risk of unauthorised access.**
  - **Access was not appropriately approved – access to key systems should be appropriately approved to prevent inappropriate access being granted.**

- Endpoint security - common weaknesses included:

  - **Unauthorised applications are not prevented – malicious applications could successfully compromise entities' systems and information.**
  - **Vulnerability management was ineffective – systems that are not regularly scanned and patched to fix known vulnerabilities are more susceptible to compromise.**
  - **Unsupported systems – key business systems and operating system software were no longer supported by vendors and were therefore not receiving updates designed to fix known vulnerabilities.**

- Human resource security - common weaknesses included:

  - **Inadequate background screening – without fit-for-purpose background screening processes, entities may engage unsuitable individuals (staff or contractors) to positions of trust, increasing insider threat risks.**
  - **Lack of security awareness training – regular cyber security education creates a culture of awareness that helps prevent social engineering attacks such as phishing and business email compromise.**
  - **Exit procedures were not completed – not completing exit procedures can contribute to unauthorised access to entities' premises, systems and information. This may also increase post-employment integrity risks such as the use or disclosure of confidential information.**

- Network security - common weaknesses included:

  - **A lack of controls to block unauthorised devices on the physical network – unauthorised devices can spread malware or be used to eavesdrop on communications or access sensitive information.**
  - **Firewall configurations were not reviewed – reviews help to identify and promptly correct exploitable configuration weaknesses. Firewalls are important security systems that control and protect networks against cyber intrusions.**

- **Networks were not segregated – segregation controls to prevent lateral movement between network segments have not been implemented. Without proper network segregation a cyber breach would be difficult to contain.**

- Information security framework - common weaknesses included:

  - **Information and cyber security policies did not exist or were outdated – without fit-for-purpose policies, entities' information security objectives are less likely to be achieved.**
  - **Lack of IT strategy – an IT strategy is crucial for informing decisions about technology and cyber security investments and implementation. The strategy should align technology and cyber security initiatives with business objectives.**
  - **Data loss prevention controls were missing or inadequate – the inadvertent or malicious leakage of information may go undetected and lead to reputational damage.**

- Business continuity - common weaknesses included:

  - **Missing or outdated continuity plans – delivery of services to the community may experience prolonged outages if adequate continuity plans do not exist.**
  - **Plans were not tested – continuity plans must be regularly tested to confirm they can meet recovery expectations.**
  - **Lack of backup restoration testing – entities should regularly restore their backups to ensure complete systems can be recovered to a common point. Business-as-usual recovery of files is not sufficient.**

- IT operations- common weaknesses included:

  - **IT asset registers were poorly maintained and stocktakes not performed – inadequate management of IT assets can result in loss or theft, leading to financial loss and reputational damage.**
  - **Service level agreements were not in place or monitored – a lack of or poorly monitored service level agreements could result in substandard services.**

- Physical security - common weaknesses included:

  - **Access to equipment enclosures/rooms was not controlled – access to equipment enclosures should be authorised, recorded and reviewed to reduce malicious or unintentional damage to IT equipment. Additional controls may include access alarms or CCTV.**
  - **Dedicated server rooms were not well maintained – server rooms need to be clear of unwanted material and cabled tidily to reduce the likelihood of damage to infrastructure.**

- Change management - common weaknesses included:

  - **Change management processes were not documented or not followed – this increases the chance of errors or delays when implementing changes and the likelihood of disruptions and outages.**

- Risk management - common weaknesses included:

  - **IT risk registers not in place or not maintained – IT risks may not be effectively managed without adequate documentation.**

- **IT risks not reviewed – timely review of risks is important to ensure mitigation strategies are cost efficient and operate effectively.**

An assessment has been made of how the Shire of Coolgardie compares with the issues and recommendations, detailed below:

OAG Recommendation	SoC Compliant – completely or partially?	SoC comments on becoming compliant, timeframes, resource implications
Access management - To ensure only authorised individuals have access, entities should:		
a. implement effective access management processes	Compliant	The shire uses a mixture of Microsoft services and physical security measures for effective access management.
b. regularly review active user accounts	Non-compliant	Accounts are managed ad-hoc.
c. enforce strong passphrases/passwords and phishing-resistant multi-factor authentication	Compliant.	The shire enforces complex password policies across the organisation. Regular phishing campaigns are performed, along with MFA for all remote access to critical systems.
d. limit and control administrator privileges	Partial.	The shire relies on administrative privileges being controlled by Integrated ICT, while Synergy administrators permissions are maintained internally.
e. implement automated access monitoring processes to detect malicious activity	Compliant	SIEM and EDR are implemented across the organisation looking for malicious activity.
Endpoint security - Entities should:		
a. implement effective controls against malware	Compliant.	The shire employs the use of SentinelOne and Rocket Cyber SIEM for endpoint protection.
b. promptly identify and address known vulnerabilities	Non-compliant	Application control is not deployed across the shire environment.
c. control installation of software on workstations, servers and mobile devices	Patial.	Integrated ICT control the installation of all software on servers/remote desktop environment. While there is ability to install software on local workstations and mobile devices.
d. prevent unapproved applications and macros from executing	Non-Compliant	Improvement item to be considered. Application control, including macro control is not enabled in the environment.
e. enforce minimum baseline controls for personal or third-party devices connecting to their systems	Partial.	Authentication is required to access shire data by any end point on the network. No specific controls are in place preventing end points from attaching to the network.
f. implement controls to prevent impersonations and detect/prevent phishing emails	Compliant	Controls are in place. The shire utilise 3rd party services for email protection, including abilities such as Phishing

		prevention/detection, impersonation prevention/detection.
g. review and harden server and workstation configurations.	Partial	Improvements such as bit-locker to be considered by the shire. Workstations, although not running administrator accounts by default, have further mechanisms available to be implemented such as Intune/bit-locker. Servers are fully restricted.
Human resources security - Entities should ensure that:		
a. pre-employment screening is conducted for key positions	Partial	Not on all occasions
b. confidentiality/non-disclosure requirements are in place and understood by individuals	Compliant	Confidential requirements are included in letter of award and/or employment contracts.
c. termination procedures are in place and followed to ensure timely access cancellation and return of assets	Compliant	Yes
d. ongoing security awareness training programs are in place and completed by all staff.	Partial – Unsure of In-house training if any.	4 Phishing and awareness campaigns are run per year which simulate phishing e-mails to a designated target group. Training is then provided to the required staff to teach the around the risks and how to identify phishing e-mails along with protecting from cyber threats.
Network security - Entities should:		
a. implement secure administration processes for network devices	Compliant	All network devices are managed with secure methods of authentication.
b. regularly review their network security controls through penetration tests	Non-compliant.	No Penetration tests have been performed – this service is available through IT provider
c. segregate their network	Compliant	All offices and data networks segregated appropriately.
d. prevent unauthorised devices from connecting to their network	Non-compliant.	
e. adequately secure wireless networks	Compliant	Wifi networks are segregated for guest access and appropriate security mechanisms in place for shire staff accessed wifi.
Information security framework - Entities should:		
a. maintain clear information and cyber security policies and governance structures to oversee and direct IT operations and cyber security	Non- compliant	Shire to implement internal governance structures relating to IT operations and Cyber Security.
b. conduct regular assessments or gain comfort through assurance reports	Non-compliant.	
c. obtain and review service organisation controls (SOC2) report or equivalent when they use software-	Non-compliant.	

as-a-service (SaaS) application for key systems including		
d. classify information and implement data loss prevention controls	Compliant	Backup of Data is implemented across organisation with indication of key data stores and backup retention and frequency periods.
Business continuity		
Entities should maintain up-to-date business continuity, disaster recovery and incident response plans and regularly test them.	Non-compliant	The Shire of Coolgardie as an outdated Disaster Recovery and Business Continuity plan. A refreshed and revised version is recommended.
IT operations - Entities should:		
a. implement appropriate IT incident management processes	Compliant	3rd Party ID provider has a detailed IT Incident Management Response plan and Process that highlights key activities and milestones per incident. This model is followed per incident experienced.
b. regularly monitor supplier performance	Compliant	A Monthly Report is provided to the Shire of Coolgardie monitoring Performance of the ticketing and support services.
c. perform regular reviews of inventory assets	Partial	The Shire of Coolgardie has access to an asset inventory that highlights workstations servers if applicable.
d. have formal service level agreements with suppliers.	Compliant	The Shire of Coolgardie has Service Level Agreements associated with the IT Support being provided.
Physical security - Entities should:		
a. implement effective physical access controls to prevent unauthorised access	Partial	IT Infrastructure is stored in locked rooms which is accessible only to staff
b. maintain environmental controls to prevent damage to IT infrastructure arising from heat, moisture, fire and other hazards	Compliant	Air con, structural integrity etc
c. gain assurance that third-party providers manage their data centres appropriately	Compliant	Appropriate Data Centre management can be provided to the Shire of Coolgardie when requested.
Change management - Entities should:		
a. consistently apply change control processes when making changes to their IT systems	Compliant	All requests for IT change need to be approved by the Director Governance and Admin other than CEO requests.
b. assess and test changes before implementation to minimise errors	Compliant	Third Party IT provider test and control the rollout of any changes prior to being introduced into the greater environment.
c. maintain change control documentation	Non-Compliant	
d. implement controls to detect unauthorised changes.	Non –Compliant	No systems are in place to detect unauthorized changes.
Risk management - Entities should:		
a. understand their information assets and apply controls based on their value	Partial	Needs to be reviewed
b. ensure IT, information and cyber security risks are identified, assessed and treated within appropriate timeframes	Compliant	The Shire utilise the 3rd Parry IT provider for best practice and correct priority on IT, Information and Cyber-Security risks.

c. provide executive oversight and remain vigilant against the risks of internal and external threats.	Compliant	3rd Party IT Provider provides detail and any industry updates as it pertains to Cyber Security risks.

CONSULTATION

Integrated ICT

Director Governance and Administration

STATUTORY ENVIRONMENT

NIL

POLICY IMPLICATIONS

Where necessary, relevant policies and procedures will be reviewed and updated to give effect to the OAG findings and recommendations.

FINANCIAL IMPLICATIONS

Unclear at the date of this report, but if there are costs to be incurred in implementing relevant policies and procedures, unable to be absorbed through current budget allocations, the CEO will report to Council accordingly.

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

Nil

VOTING REQUIREMENT

Simple Majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That the CEO give effect to implementing, where necessary, in a timing and cost-effective manner, the findings and recommendations of the OAG Report - Local Government 2022-23 – Information Systems Audit Results, and where appropriate, report back to Council, via the Audit Committee on issues and implications.

5.1.6 WORKPLACE HEALTH AND SAFETY REPORT

Location: **Shire of Coolgardie**

Applicant: **Nil**

Disclosure of Interest: **Nil**

Date: **10 July 2024**

Author: **Kathy Brooking, Leisure & Recreation Development Manager**

SUMMARY

That the Audit Committee receive the Workplace Health and Safety Compliance Schedule and the Workplace Health and Safety Management Review in terms of progress.

BACKGROUND

Shire staff have been working in consultation with Nicole Tynan from HSE Collective within the area of Workplace health and Safety across the organisation.

COMMENT

Compliance to WHS Act and Regulations requires the Shire to maintain records and processes in accordance with the Act. Ensuring safety of staff, contractors and public is a primary responsibility and role of the Shire.

CONSULTATION

Shire Staff

Contractors

HSE Collective

STATUTORY ENVIRONMENT

Nil

POLICY IMPLICATIONS

Nil

FINANCIAL IMPLICATIONS

Nil

STRATEGIC IMPLICATIONS

Accountable and effective leaders

High quality corporate governance, accountability and compliance

ATTACHMENTS

1. **WHS Inspection and Compliance Schedule - Confidential**
2. **WHS Management Review - Confidential**

VOTING REQUIREMENT

Simple majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That the Audit Committee RECEIVE the Workplace Health and Safety Inspection and Compliance Schedule and Workplace Health and Safety Management Review Report.

5.2 Operation Services

5.2.1 CEO CREDIT CARD LISTING FROM FEBRUARY 2024 TO MAY 2024

Location: **Nil**

Applicant: **Nil**

Disclosure of Interest: **CEO, James Trail has a financial interest in this item. In accordance with section 5.70(2) of the Local Government Act 1995, I declare a financial interest in the agenda item List of credit card payments. The interest is in relation to CEO credit card vouchers.**

Date: **9 July 2024**

Author: **Sachin Kumar, Senior Finance Officer**

SUMMARY

For the Audit Committee to receive the list of credit card payments from February 2024 to May 2024 for the Chief Executive Officer.

BACKGROUND

The Local Government (Financial Management) Regulations 1996, Regulation 13(3)(b) requires that Council receive a list of credit cards paid in the month, and that this be recorded in the minutes. Council has delegated to the Chief Executive Officer that authority to make these payments from the Municipal and Trust Funds.

COMMENT

The schedule of payments made under delegated authority as summarised below and recommended to be received by the audit committee, has been checked and is supported by vouchers and invoices which have been duly certified as to the receipt of goods and provision of services, and verification of process and costings.

It is deemed prudent that all Chief Executive Officer credit card vouchers now be presented to the Audit Committee for consideration and recommendation to Council. This is particularly the case given the authorisation required for the Chief Executive Officer credit card.

CONSULTATION

Nil

STATUTORY ENVIRONMENT

Local Government (Financial Management) Regulations 1996, Regulation 13 – List of Accounts.

POLICY IMPLICATIONS

CS-PROCUREMENT POLICY. Policy CS-11 as amended, sets the guides with regards to the purchase of goods or services provided.

FINANCIAL IMPLICATIONS

Nil

STRATEGIC IMPLICATIONS

Accountable and effective leaders

Maintain integrated strategic and operational plans

ATTACHMENTS

1. CEO Credit Card Listings From February 2024 To May 2024

VOTING REQUIREMENT

Simple majority

AUDIT COMMITTEE RESOLUTION AND OFFICER RECOMMENDATION

That the Audit Committee,

1. Accept listing (attached) of credit card invoices totalling $17,068.23 paid from February 2024 to May 2024 by the Chief Executive Officer under delegated authority of Council.

2. Recommend the Council receive the listing of credit card invoices totalling $17,068.23 paid from the period February 2024 to May 2024 by the Chief Executive Officer under delegated authority.

3. Recommend to Council the Shire President authorise the credit card vouchers totalling $17,068.23 paid from the period February 2024 to May 2024 by the Chief Executive Officer under delegated authority.

6 NEW BUSINESS OF AN URGENT NATURE INTRODUCED BY DECISION OF MEETING

6.1 Elected Members

6.2 Shire Officers

7 CLOSURE OF MEETING