Shire of Broome
A future, for everyone

AGENDA

FOR THE

AUDIT AND RISK COMMITTEE MEETING

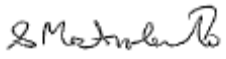
28 AUGUST 2024

NOTICE OF MEETING

Dear Council Member,

The next Audit and Risk Committee of Council will be held on Wednesday, 28 August 2024 in the Council Chambers, Corner Weld and Haas Streets, Broome, commencing at 10am.

Regards,



S MASTROLEMBO
Chief Executive Officer

20/08/2024

Our Mission

"To deliver affordable and quality Local Government services."

DISCLAIMER
The purpose of Council Meetings is to discuss, and where possible, make resolutions about items appearing on the agenda. Whilst Council has the power to resolve such items and may in fact, appear to have done so at the meeting, no person should rely on or act on the basis of such decision or on any advice or information provided by a Member or Officer, or on the content of any discussion occurring, during the course of the meeting.

Persons should be aware that the provisions in section 5.25 of the *Local Government Act 1995* establish procedures for revocation or rescission of a Council decision. No person should rely on the decisions made by Council until formal advice of the Council decision is received by that person. The Shire of Broome expressly disclaims liability for any loss or damage suffered by any person as a result of relying on or acting on the basis of any resolution of Council, or any advice or information provided by a Member or Officer, or the content of any discussion occurring, during the course of the Council meeting.

Should you require this document in an alternative format please contact us.

SHIRE OF BROOME

AUDIT AND RISK COMMITTEE MEETING

WEDNESDAY 28 AUGUST 2024

INDEX – AGENDA

1. OFFICIAL OPENING

2. ATTENDANCE AND APOLOGIES

Elected Members:	C Mitchell	Shire President
	Cr. D Male	Deputy Shire President
	Cr. M Virgo	
Officers:	Mr. S Mastrolembo	Chief Executive Officer
	Mr. J Hall	Director Infrastructure
	Ms. K MacClure	Acting Director Corporate Services
	Mr. K Williams	Director Development Services
	Mr. R Ali	Manager Information Services
	Ms. R Doyle	Manager Governance, Strategy and Risk
	Ms. E French	Manager Financial Services

Invited:

Office of the Auditor General:	Mr. P Tilbrook
	Ms. A Morrissey
RSM Australia:	Mr. A Neo

3. DECLARATIONS OF FINANCIAL INTEREST / IMPARTIALITY

4. CONFIRMATION OF MINUTES

RECOMMENDATION:

That the Minutes of the Audit and Risk Committee held on 22 April 2024, as published and circulated, be confirmed as a true and accurate record of that meeting.

5. REPORT OF OFFICERS

5.1 PERFORMANCE AUDIT - PHYSICAL SECURITY OF SERVER ROOM ASSETS 2024

LOCATION/ADDRESS:	Nil
APPLICANT:	Nil
FILE:	COA01
AUTHOR:	Project Officer
CONTRIBUTOR/S:	Manager Information Services
RESPONSIBLE OFFICER:	Acting Director Corporate Services
DISCLOSURE OF INTEREST:	Nil

SUMMARY:

The Audit and Risk Committee is presented to examine the:

a) 2024 Performance Audit – Local Government Physical Security of Server Room Assets Emerging Findings Letter; and
b) Office of Auditor General Local Government Physical Security of Server Assets Performance Audit Report.

BACKGROUND

Previous Considerations

Nil.

The Office of the Auditor General (OAG) conduct performance audits to assess the efficiency and effectiveness of public sector activities, services and programs. These audits highlight issues surrounding regulatory, financial and administrative processes and can also highlight best practice approaches for all entities to consider implementing.

Topics for audit are selected by the Auditor General, and may include request for audit from Parliament, the government or broader community.

Results of the audit are tabled in Parliament and published on the OAG website.

COMMENT

A Performance Audit of 16 non-metropolitan local government entities was undertaken by the OAG to assess whether each local government effectively managed their server assets to protect them from physical and environmental hazards.

OAG officers attended the Shire of Broome on 23 April 2024 to inspect the Shire's physical server room assets. Each local government received an Emerging Findings Letter which contained specific findings to the local government and a draft of the Summary of Findings Report summarising all of the 16 local government findings.

A copy of the Emerging Findings Letter and draft Summary of Findings Report delivered to the Shire of Broome is presented in Confidential Attachment 1 for the Audit and Risk Committee to examine. Details contained within the Emerging Findings Letter are considered confidential as releasing them publicly would increase the likelihood that identified risks could be the target of fraudulent or illegal activities.

The Summary of Findings Report was tabled in State Parliament under sections 24 and 25 of the *Auditor General Act 2006* and a copy of the final OAG Performance Audit Report - Local Government Physical Security of Server Assets is presented in Attachment 2 of this report.

CONSULTATION

Office of the Auditor General

STATUTORY ENVIRONMENT

Local Government Act 1995

7.12A (3) Duties of local government with respect to audits

(3) A local government must —

(aa) examine an audit report received by the local government; and

(a) determine if any matters raised by the audit report, require action to be taken by the local government; and

(b) ensure that appropriate action is taken in respect of those matters

POLICY IMPLICATIONS

Nil.

FINANCIAL IMPLICATIONS

No Audit fees were payable to the OAG for the audit. Unlike financial audits, performance audits are funded by the OAG via parliamentary appropriation.

Remediation of issues raised within the report may require budget allocations to resolve. Where this requires funding outside of the existing 2024/2025 adopted annual budget, Responsible officers would request budget allocations either through the Shire's Finance and Costing Review process, or as part of the 2025/2026 annual budget process.

RISK

The audit findings provide management with recommendations particularly to strengthen internal controls and reduce the likelihood of certain risks. Delays in progressing and completing the audit findings can be unfavourable to the organisation, but are also weighed against other demands on Shire resources, and the costs to the community.

STRATEGIC ASPIRATIONS

Performance	**We will deliver excellent governance, service & value for everyone.**
Outcome 14	***Excellence in organisational performance and service delivery***
Objective	14.1 Embrace best practice approaches and new innovations to improve business efficiencies and the customer experience.
Objective	14.2 Deliver fit for purpose facilities and equipment.
Objective	14.3 Monitor and continuously improve performance levels.

VOTING REQUIREMENTS
Simple Majority

REPORT RECOMMENDATION:

That the Audit and Risk Committee recommends that Council:

1. *Receive the 2024 Performance Audit – Local Government Physical Security Server Room Assets Emerging Findings Letter as per* ***Confidential Attachment 1****;*
2. *Receive the Office of Auditor General - Local Government Physical Security of Assets Performance Audit Report; and*
3. *Requests the Chief Executive Officer to progress the finalisation of outstanding Emerging Findings as soon as practicable.*

Attachments

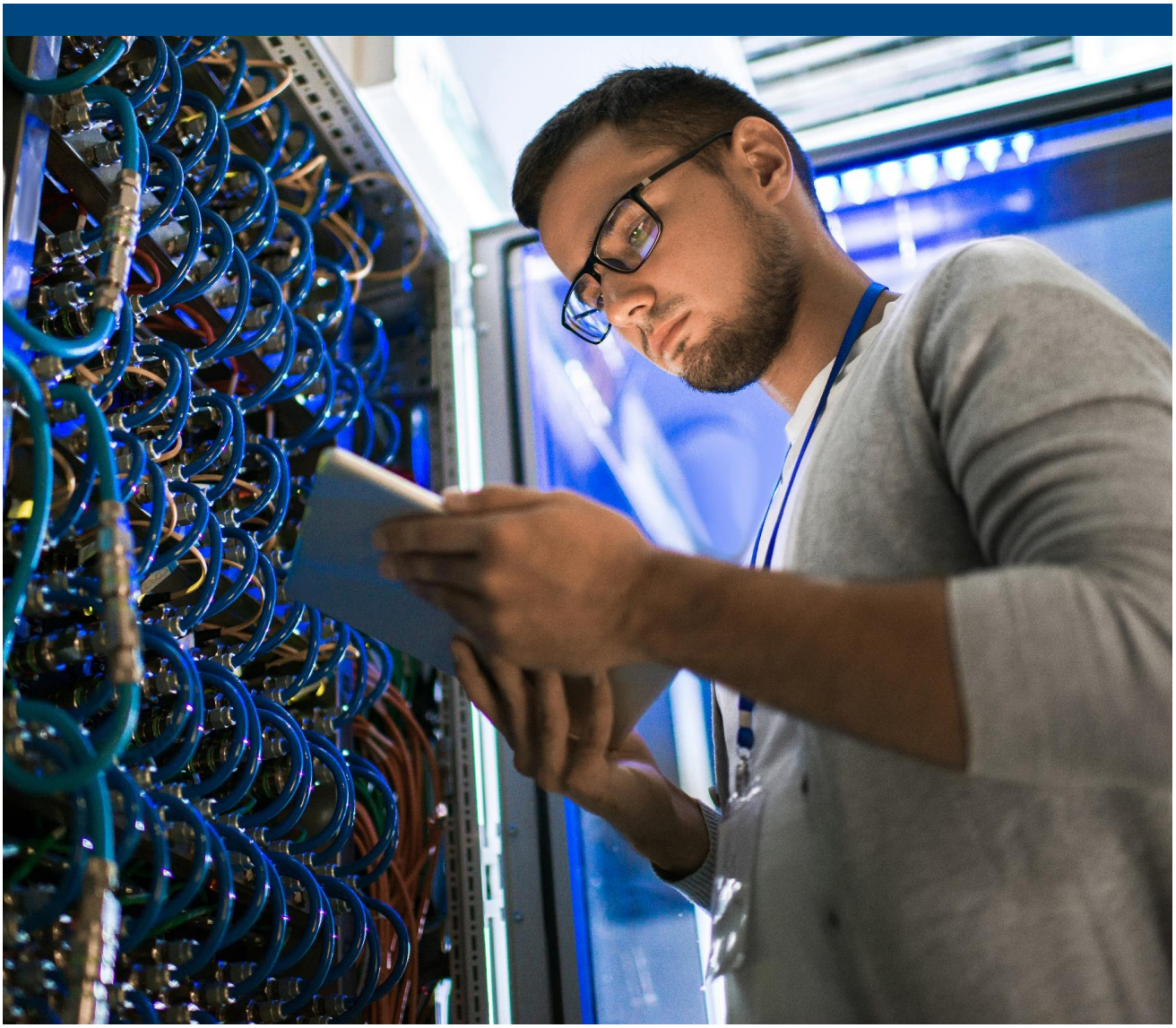
1. 2024 Performance Audit Local Government Physical Server Room Assets (Emerging Findings Letter and Summary of Findings Report) *(Confidential to Councillors and Directors Only)*
   This attachment is confidential in accordance with section 5.23(2) of the Local Government Act 1995 section 5.23(2)((f)(ii)) as it contains "a matter that if disclosed, could be reasonably expected to endanger the security of the local governments property".
2. OAG Performance Audit Report - Local Government Physical Security of Server Assets.

Office of the Auditor General
Serving the Public Interest

Report 20: 2023-24 | 24 June 2024

PERFORMANCE AUDIT

Local Government Physical Security of Server Assets



Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Adam Dias
Paul Tilbrook
Talia Channer
Lyndsay Fairclough
Information Systems Audit team

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

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: shutterstock.com/SeventyFour

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government Physical Security of Server Assets

Report 20: 2023-24
24 June 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT PHYSICAL SECURITY OF SERVER ASSETS

This report has been prepared for submission to Parliament under the provisions of sections 24 and 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 whether 16 non-metropolitan local government entities of varying sizes effectively manage access to server assets and protect them from environmental hazards.

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

Caroline Spencer
Auditor General
24 June 2024

Contents

Auditor General's overview

Many local government entities rely on server assets to run their information technology (IT) systems and applications that are integral to their operations. These server assets need to be protected against physical and environmental hazards that can disrupt continuous IT service and the delivery of services to the community.

All 16 local government entities in this audit had physical server assets located onsite, but each had their own unique IT needs, risks and resources. It was encouraging to find that all the audited local government entities had some protections in place to restrict physical access to their server assets and reduce the risk of accidental or malicious damage. They had also taken steps to reduce the impact of environmental hazards such as high temperatures and humidity on these assets. However, we found many audited local government entities could better use and maintain the protections they have and improve their monitoring of hazards.

We have raised similar issues in our previous information systems audits of local government entities. Most recently, our 2022-23 information systems audits found 45% of the local government entities we tested needed to improve the physical security of their server assets.[1]

This report includes recommendations and better practice principles that local government entities of all sizes can use to protect their server assets against damage.

[1] Office of the Auditor General, *Local Government 2022-23 – Information Systems Audit Results*, OAG, 27 May 2024.

Executive summary

Introduction

This audit assessed whether 16 non-metropolitan local government entities (entities) of varying sizes effectively manage access to server assets and protect them from environmental hazards. The entities were from the Gascoyne, Goldfields, Great Southern, Kimberley, Pilbara and Wheatbelt regions.

Detailed findings were provided to each entity. However, we have anonymised findings throughout this report to not compromise the security and continuity of their systems and information.

Background

Entities rely on server assets to run key IT systems and applications. Our 2022-23 local government information systems audits found a substantial proportion (45%) of the entities we tested needed to improve the physical security of these assets.[2] Inadequate protections can lead to accidental or malicious damage; compromising the security of an entity's information and its ability to maintain continuous IT service.

Server assets include the entities' servers, as well as storage devices and network equipment. These assets provide shared access to applications, such as web pages, email and back office systems that are integral to the delivery of services to the community. In this report we have used the term server room to describe where the server assets are housed, whether this is in a dedicated server room or a shared space.

There are several actions entities can take to protect their server assets (Appendix 1). Server assets should be mounted in specialised enclosures called a rack. These racks protect the assets, channel airflow, and include cable management systems. Some racks can also include power distribution and protection, cooling fans and sensors for monitoring temperature and humidity.

It is good practice to house racks in a dedicated server room. However, when this is not possible, and server assets are housed in shared spaces, they require additional controls such as cages to prevent unauthorised access.

To protect server assets, the rooms and racks should have the following:

- access controls to prevent malicious or accidental damage
- fire detection and suppression to limit fire damage
- power filtering and redundancy through uninterruptible power supplies (UPS[3]). This may be augmented with a generator
- room or rack-based cooling to remove heat generated by the server assets
- environmental sensors throughout the room to measure temperature and humidity and issue alerts when these vary beyond acceptable limits
- cable management systems to improve access, workplace safety, fault detection and airflow within a rack.

[2] Office of the Auditor General, *Local Government 2022-23 – Information Systems Audit Results*, OAG, 27 May 2024.

[3] A UPS is a device containing batteries that provides backup power and protection to server assets when the mains power fails or fluctuates.

Conclusion

All 16 audited entities had controls to partly protect their server assets from unauthorised access and environmental hazards. Despite the audited entities' different IT requirements and facilities, most need to better protect their server assets.

Half the audited entities need to improve their storage and tracking of the keys that give access to server assets. While all entities used racks, only four made appropriate use of them. Twelve entities had racks that were missing panels or had unlocked doors unnecessarily exposing the server assets to damage from anyone passing through the server room.

All audited entities had some environmental controls in place to cool their server assets, extinguish a fire and manage power interruptions. However, most did not service or test all their controls to ensure they worked as expected. Concerningly, nine did not have adequate systems to alert them of a fire in the server room, or in some cases, anywhere in the building. Only three entities appropriately monitored their server room environment for high temperature and humidity.

Key findings

The entities we visited had varying approaches to storing and securing their server assets, reflecting the different IT needs and the available facilities. Five entities had dedicated server rooms, only accessible by selected staff. Eight entities kept their server assets in multipurpose rooms accessible to all staff with no public access. The other three entities stored their server assets in areas that were accessible by the public.

Entities can better control access to their server assets

While most entities had taken steps to protect server assets, more can be done to tighten access and reduce the risk of both accidental and malicious damage.

Keys are not always well managed

Half of the audited entities need to improve how they store and track the keys that grant access to server rooms and racks. While all had installed locks to help secure their server assets, including some with electronic systems (Case study 1), common issues we found included:

- Physical keys kept in easily accessed areas such as office drawers, in the rack door lock, or on pegs next to the server rack.
- A record of who used physical keys to access server assets was not maintained. Without this kind of record, entities cannot easily track when physical keys are used and returned.
- A lack of policy or procedure to help guide staff on key allocation and usage.

Locks on server rooms and racks are effective ways to control access, but their success depends on proper key management.

Case study 1: Electronic locks

Electronic access locks offer advantages over traditional, physical keys. As they grant access using a code or swipe card instead of a physical key, entities can quickly and easily allocate and revoke access. Further, as these systems keep an entry log, entities can easily track who has unlocked the room.

Four of the entities had installed these systems.

Source: OAG

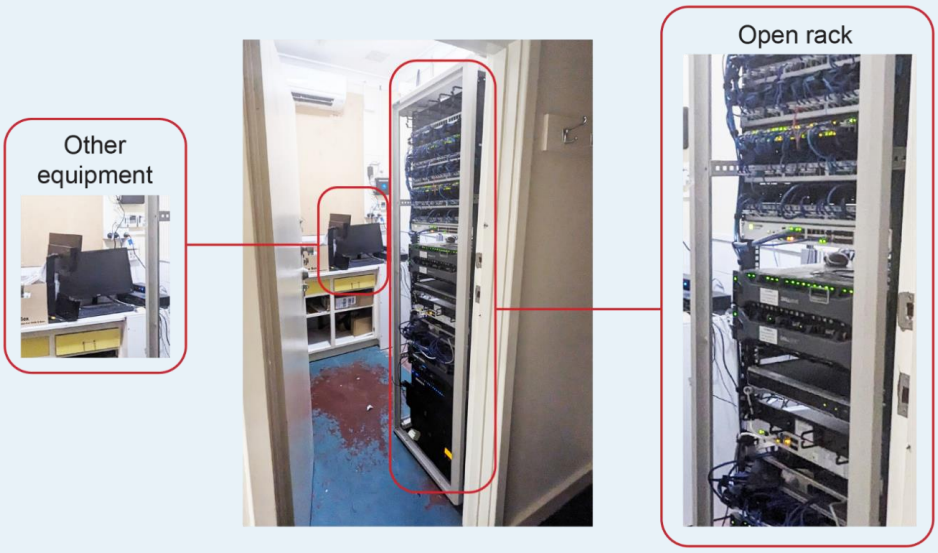
Figure 1: Photo of electronic lock

Servers, network devices and cabling were exposed

All entities used server racks, but only four made appropriate use of them. Twelve entities had racks with missing panels or unlocked doors (Case study 2). One of these entities had installed a rack that was too small for their server and as the asset extended beyond the frame, the door could not be attached. In some cases, we observed the missing panels being stored nearby. If the server assets are not enclosed, they are exposed to unauthorised

access that can lead to accidental or malicious damage from anyone passing through the area.

Case study 2: Open rack risks damage



Source: OAG

Figure 2: Photo of rack with no panels

One entity had not enclosed its server assets at all.

While the rack was kept in a locked room, the room was also used to store other equipment. This meant staff accessed the room for various reasons, exposing the server to increased traffic and risk of accidental damage.

Server assets could be better protected against heat, moisture, fire and other environmental hazards

All entities' server rooms had some environmental controls in place to cool their server assets, extinguish a fire and manage power interruptions. More can be done to monitor emerging hazards and service environmental controls.

Detection of environmental hazards could be improved

Nine entities did not have adequate fire alert systems. This included not having smoke detectors in their server room or anywhere in the building, and smoke detectors that were not monitored externally. A lack of warning systems delays response and places server assets and office staff at increased risk.

Only three entities monitored the temperature and humidity of their server rooms. Monitoring room conditions is important as inappropriate temperatures or excessive humidity can lead to poor performance and damage to server assets. We note that 10 entities did monitor the internal temperature of their server assets.

While all the entities had a UPS, four were not monitoring the unit to be warned of power irregularities. Failure to monitor may not give the entity enough time to gracefully shut down

its server assets prior to losing power which may result in information loss or equipment damage.

Environmental controls were not regularly serviced

Entities did not adequately service and test their environmental controls to ensure they would work when needed (Case study 3). We found:

- only one entity regularly serviced their UPS. At three other entities the UPS or its batteries had reached the end of useful life and needed replacing
- three entities had not regularly serviced the air conditioners that kept their server assets cool
- fire extinguishers at four entities were not inspected every six months, as recommended by the Australian Standards[4].

Case study 3: Failure of power backups

During a recent power outage an entity's backup power systems failed. This damaged a critical storage device and required data and systems to be restored from backups. It took the entity three weeks to fully recover its IT systems.

While this entity had both a UPS and a generator in place to protect its server assets, these had not been adequately tested.

When the mains failed, the UPS operated as expected and supplied emergency power for a short period of time. However, the generator failed to start and once the UPS battery ran flat the server assets stopped operating.

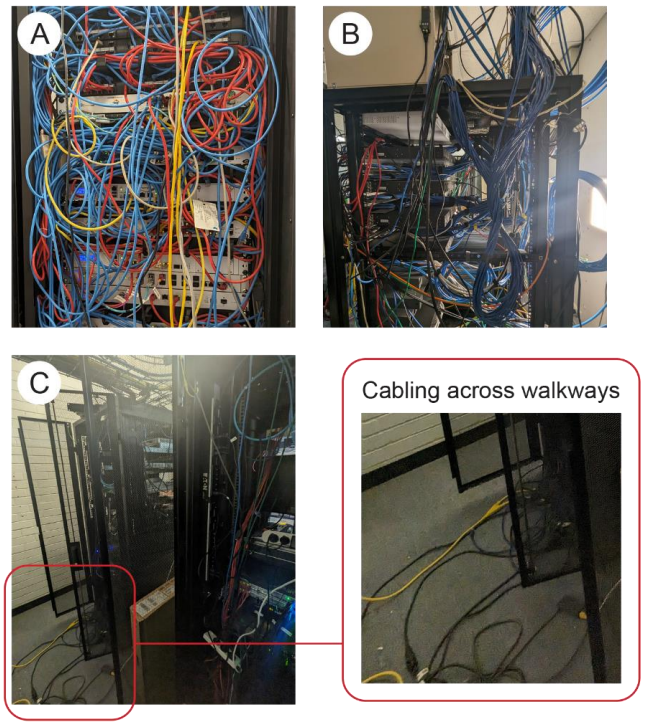
Network and power cabling could be improved

Fourteen entities did not have structured cable management or had not used this effectively. Structured cabling is a system of cable ties and supports that minimise the risk of hazards posed by uncontrolled cables. We observed:

- excessive cabling within the racks, which may restrict airflow to cool the server assets and increase time to diagnose issues (Figure 3, A)
- unsupported cables which may wear electrical connectors and cause failures (Figure 3, B)
- cabling across walkways which create tripping hazards and may result in outages (Figure 3, C).

Disorganised cabling can cause accidents, outages or additional wear and tear on the server assets.

[4] AS1851-2012 Routine service of fire protection systems and equipment.



Source: OAG

Figure 3: Photos of poor cabling

Server rooms are not kept clear of other hazards

Seven entities have not appropriately managed risks when storing other items in their server rooms or near their server assets when these are housed in a multipurpose room (Case study 4). We observed:

- flammable or explosive items, such as cardboard and pressurised containers, stored close to and between racks
- boxes blocking the air conditioner
- dust building up on server assets which can cause overheating, static electricity and damage the assets.

Other items should be kept to a minimum and stored appropriately, and the room kept clean to reduce the likelihood of damage from fire, pests, overheating and electrical issues.

Case study 4: Excess items stored in the room could increase the risk and extent of a fire

Source: OAG

Figure 4: Photo of high risks items stored in the server room

One entity stored an excessive amount of non-server related items including wood and cardboard in the server room. Better practice would be to minimise storage in the server room to reduce the likelihood and extent of a fire.

Recommendations

The 16 audited entities should consider the key elements outlined in Appendix 1 to manage access and protect the physical security of their server assets. In particular:

1. Improve their physical security access controls to prevent accidental and malicious damage to their server assets. Consideration should be given to:
    a. management of keys to ensure only approved staff can access the server assets and access is logged and monitored
    b. use of racks to fully enclose server assets
    c. additional physical controls where racks are accessible to the public.
2. Improve their environmental controls to protect server assets by:
    a. implementing and monitoring environmental changes such as fire, temperature and humidity
    b. regularly servicing all environmental controls
    c. implementing structured cable management
    d. minimising or better managing the storage of other items around or near their server assets.

In accordance with section 7.12A of the *Local Government Act 1995*, the 16 audited local government entities should prepare a report on any matters identified as significant to them for submission to the Minister for Local Government within three months of this report being tabled in Parliament, and within 14 days of submission publish it on their website.

Response from the audited entities

Audited entities generally accepted the recommendations and confirmed that where relevant, they will improve their controls to better protect their server assets against unauthorised access and environmental hazards.

Audit focus and scope

This audit assessed whether 16 non-metropolitan local government entities effectively manage access to server room assets and protect them from environmental hazards. The entities were from the Gascoyne, Goldfields, Great Southern, Kimberley, Pilbara and Wheatbelt regions.

Our criteria were:

- Are server room assets protected from unauthorised access?
- Are appropriate environmental controls in place to protect server rooms?

We visited each entity and:

- reviewed policies and procedures
- conducted interviews with key staff
- carried out physical inspection of server rooms and environmental controls
- examined relevant documents and records.

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 $288,500.

Appendix 1: Better practice principles – key elements of physical security of server assets

The table below shows key elements to help manage access and protect the physical security of server assets. These elements are not exhaustive and entities should assess their own physical security needs.

Key elements	Description
Policies and procedures	Policies and procedures identify the server assets that need protection and how the risk of damage, compromise or loss will be minimised. Areas to consider include: • access to server rooms and racks • environmental controls including their servicing and monitoring • server room upkeep. Policies should be easily accessible by staff, clearly outline roles and responsibilities and detail appropriate record keeping.
Access controls	Only authorised staff should have access to server assets. Access controls restrict and manage who can access server assets and include: • physical barriers to entry to the server racks and room. Server assets should be suitably secured and enclosed • user access management. Allocated keys, cards and fobs should be stored securely and tracked. Access should be removed when an individual's employment or engagement ends or they have a change in role • routinely checking access to identify instances of unauthorised entry.

Environmental controls	Environmental controls protect server assets from environmental hazards and can include:
	• UPS and backup generators to provide emergency power in the event of a power failure
	• rack based cooling (fans) or room air conditioning to prevent overheating
	• fire detection and suppression to limit fire damage
	  ○ fire detection can include smoke detectors and very early smoke detection apparatus (VESDA)
	  ○ fire suppression can include fire extinguishers, dry pipe sprinkler systems and gas suppression systems
	• room sensors to detect water and measure if temperature and humidity vary beyond acceptable limits.
	Environmental controls should be regularly serviced and tested to ensure they will work when needed.

Server racks	Server racks provide a framework to protect and organise server assets. Entities should install racks that meet their individual needs including the type of facility, available space and the size, power, cooling and cabling requirements of server assets. Server racks should be kept locked to prevent unauthorised access. Racks can come preconfigured with power protection and distribution, cooling, cable management and environmental monitoring.
Cable management	Cable management systems improve access to server assets and fault detection and airflow within a rack. Cables should be appropriately labelled, colour coded and secured using structured cabling.

Source: OAG

Auditor General's 2023-24 reports

Number	Title	Date tabled
20	Local Government Physical Security of Server Room Assets	24 June 2024
19	Local Government Management of Purchasing Cards	12 June 2024
18	Local Government 2022-23 Financial Audit Results	6 June 2024
17	Local Government IT Disaster Recovery Planning	31 May 2024
16	Local Government 2022-23 – Information Systems Audit Results	27 May 2024
15	Government Campaign Advertising	15 May 2024
14	State Government 2022-23 – Information Systems Audit	12 April 2024
13	Provision of Supplementary Information to the Standing Committee on Estimates and Financial Operations – Opinions on Ministerial Notifications	5 April 2024
12	Digital Identity and Access Management – Better Practice Guide	28 March 2024
11	Funding for Community Sport and Recreation	21 March 2024
10	State Government 2022-23 – Financial Audit Results	20 December 2023
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Local Government 2021-22 – Financial Audit Results	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

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

5.2 INTERIM AUDIT 2023/2024	
LOCATION/ADDRESS:	Nil
APPLICANT:	Nil
FILE:	COA01
AUTHOR:	Project Officer
CONTRIBUTOR/S:	Manager Financial Services
RESPONSIBLE OFFICER:	Acting Director Corporate Services
DISCLOSURE OF INTEREST:	Nil

SUMMARY:
The Audit and Risk Committee is presented the Interim Audit Management Report for year ended 30 June 2024.

BACKGROUND

Previous Considerations

Nil.

Under section 7.9 of the *Local Government Act 1995* (the Act), an Auditor is required to examine the accounts and annual financial report submitted by a local government for audit. The Auditor is required to prepare a report by 31 December following the financial year to which the accounts and report relate and forward a copy of that report to:

(a) The Mayor or President;

(b) The Chief Executive Officer (CEO); and

(c) The Minister.

Furthermore, under Regulation 10(4) of the *Local Government (Audit) Regulations 1996* (Audit Regulations), where it is considered appropriate to do so, the Auditor may prepare a Management Report to accompany the Auditor's Report, which is also to be forwarded to the persons specified in section 7.9 of the Act.

The Auditors may in accordance with their audit plan prepare an interim audit to consider relevant components of the annual financial report.

In accordance with section 7.12A (3) of the Act, the Audit and Risk Committee (the Committee) is required to examine the reports of the Auditor after receiving a report from the CEO on the matters reported and:

- Determine if any matters raised require action to be taken by the local government; and
- Ensure that appropriate action is taken in respect of those matters.

COMMENT

The Shire's Interim Audit was conducted by RSM Australia (RSM) on behalf of the Office of the Auditor General (OAG) on 15 - 19 April 2024 and duplicate copies of the Interim Management Letter and Interim Audit Management Report were forwarded to the Chief Executive Officer and Shire President on the 23 July 2024.

A copy of the transmittal letter to the Chief Executive Officer is presented and included as Attachment 1 to this report.

The interim audit focus for the OAG was to primarily evaluate the Shire's financial control environment, and to obtain an understanding of the key business processes, risks and control relevant to the audit of the annual financial report.

The Interim Management Report for the year ending 30 June 2024 is presented and included as Confidential Attachment 2 to this report. The Interim Report details risks relating to operational controls within the Shire and includes comments from management on each issue, inclusive of details on how these matters will be mitigated. Details contained within the report are considered confidential as releasing them publicly would increase the likelihood that identified risks could be the target of fraudulent or illegal activities.

The final audit for the 2023/2024 financial year is due to commence in October, and the Auditors will issue a final year Management Report in due course. This report will reflect the status of the existing findings list as well as any newly identified findings.

CONSULTATION

Office of the Auditor General
RSM Australia

STATUTORY ENVIRONMENT

Local Government Act 1995

7.9 Audit to be conducted
In accordance with section 7.9 of the *Local Government Act 1995 (the Act)*, an Auditor is required to examine the accounts and annual financial report submitted by a local government for audit. The Auditor is required to prepare a report by 31 December following the relevant financial year and send a copy of that report to:

(a) The Mayor or President;
(b) The Chief Executive Officer (CEO); and
(c) The Minister.

Additionally, under Regulation 10(4) of the *Local Government (Audit) Regulations 1996* (*Audit Regulations*), the Auditor may, when deemed appropriate, prepare a Management Report to accompany the Auditor's Report. This Management Report is also to be forwarded to the individuals specified in section 7.9 of *the Act*.

7.12A (3) Duties of local government with respect to audits

(3) A local government must —

(aa) examine an audit report received by the local government; and

(a) determine if any matters raised by the audit report, require action to be taken by the local government; and

(b) ensure that appropriate action is taken in respect of those matters

Local Government (Audit) Regulations 1996

10 (4) Report by Auditor

(4) Where it is considered by the auditor to be appropriate to do so, the auditor is to prepare a management report to accompany the auditor's report and to forward a copy of the management report to the persons specified in section 7.9(1) with the auditor's report.

Local Government (Financial Management) Regulations 1996

POLICY IMPLICATIONS

Nil.

FINANCIAL IMPLICATIONS

Remediation of any of the issues raised within the Audit Management Report may require budget allocations to resolve. Where this requires funding outside of the existing 2024/2025 adopted annual budget, Responsible Officers would request budget allocations either through the Shire's Finance and Costing Review process, or as part of the 2025/2026 annual budget process.

Interim audit fees form part of the annual (lump sum) audit fee issued by the OAG. The Shire CEO received notice from the OAG via Letter dated 9 July 2024 (presented in Attachment 3 of this report) of an estimated increase in Audit fees for the 2023-2024 financial year to $150,200 (exclusive of GST) this is an increase of $8,160 from the prior year fees of $142,040.

A summary of the indicative median fee increases from the OAG across all local governments is also presented to the Audit and Risk Committee for its reference in Attachment 4 of this report, the Shire of Broome being a Band 2 local government has been allocated at the top end of that band. Responsible Officers will request budget allocations through the Shire's Finance and Costing Review process.

RISK

The audit findings provide management with recommendations particularly to strengthen internal controls and reduce the likelihood of certain risks. Delays in progressing and completing the audit findings can be unfavourable to the organisation, but are also weighed against other demands on Shire resources, and the costs to the community.

STRATEGIC ASPIRATIONS

Performance	**We will deliver excellent governance, service & value for everyone.**
Outcome 13	***Value for money from rates and long term financial sustainability***
Objective	13.1 Plan effectively for short- and long-term financial sustainability
Outcome 14	***Excellence in organisational performance and service delivery***
Objective	14.3 Monitor and continuously improve performance levels.

VOTING REQUIREMENTS
Simple Majority

REPORT RECOMMENDATION:

That the Audit and Risk Committee recommends that Council:

1. *Receive the Interim Audit Management Report for year ended 30 June 2024 as per Confidential Attachment 2; and*

2.	*Requests the Chief Executive Officer to progress the finalisation of all outstanding findings as soon as practicable.*

Attachments

1. Letter from OAG to Chief Executive Officer regarding 2023-2024 Interim Audit
2. Letter from OAG to CEO Attachment - Interim Audit 2023-2024 Management Report *(Confidential to Councillors and Directors Only)*
   This attachment is confidential in accordance with section 5.23(2) of the Local Government Act 1995 section 5.23(2)((f)(ii)) as it contains "a matter that if disclosed, could be reasonably expected to endanger the security of the local governments property".
3. Letter to Chief Executive Officer regarding OAG Audit Fee Changes 9 July 2024
4. Summary of OAG Amended Fee Increases Opinion Delivery Year 2024/2025

Office of the Auditor General
Serving the Public Interest

7th Floor, Albert Facey House
469 Wellington Street, Perth

Mail to: Perth BC
PO Box 8489
PERTH WA 6849

Tel: 08 6557 7500
Email: info@audit.wa.gov.au

Our Ref: 8250

Mr Sam Mastrolembo
Chief Executive Officer
Shire of Broome
PO Box 44
BROOME WA 6725

Email: Sam.Mastrolembo@broome.wa.gov.au

Dear Mr Mastrolembo

ANNUAL FINANCIAL REPORT
INTERIM AUDIT RESULTS FOR THE YEAR ENDED 30 JUNE 2024

We have completed the interim audit for the year ended 30 June 2024. We performed this phase of the audit in accordance with our audit plan. The focus of our interim audit was to primarily evaluate your financial control environment, and to obtain an understanding of the key business processes, risks and internal controls relevant to our audit of the annual financial report.

Management control issues
We would like to draw your attention to the attached listing of deficiencies in internal control and other matters that were identified during the course of the interim audit. These matters have been discussed with management and their comments have been included on the attachment. The matters reported are limited to those deficiencies that were identified during the interim audit that we have concluded are of sufficient importance to merit being reported to management.

This letter has been provided for the purposes of your local government and may not be suitable for other purposes.

We have forwarded a copy of this letter to the Shire President. A copy will also be forwarded to the Minister for Local Government when we forward our auditor's report on the annual financial report to the Minister on completion of the audit.

Feel free to contact me on 6557 7674 if you would like to discuss these matters further.

Yours faithfully

AMadnack

Aram Madnack
Acting Senior Director
Financial Audit
23 July 2024

Attach

Office of the Auditor General
Serving the Public Interest

Our Ref: 8251

7th Floor, Albert Facey House
469 Wellington Street, Perth

Mail to: Perth BC
PO Box 8489
PERTH WA 6849

Tel: 08 6557 7500
Email: info@audit.wa.gov.au

Mr Sam Mastrolembo
Chief Executive Officer
Shire of Broome
27 Weld Street
BROOME WA 6725

Email: sam.mastrolembo@broome.wa.gov.au

Dear Mr Mastrolembo

AUDIT FEE 2024

Our indicative fee for the audit of your 2023-24 financial report is $150,200 (excl. GST). The indicative fee represents an increase compared to the prior year invoiced audit fee (2022-23: $142,040).

This fee has been calculated to cost-recover the OAG's expenses to deliver the audit work program, plus any directly related costs such as contract fees and travel expenses, as applicable.

In addition to giving assurance on your entity's annual financial report, the audit will also provide transparency surrounding relevant legislative compliance, financial controls, probity, and governance matters, and enables our whole-of-sector parliamentary reporting and stakeholder liaison across the sector.

To uphold our auditor obligations, we are aiming to issue all financial audit opinions for the 2024 reporting period by no later than 6 December 2024. This will enable you to discharge your statutory financial reporting responsibility to ratepayers in a timely manner (i.e., by no later than 31 December 2024).

Increase in audit effort
In recent years there has been an increase in audit effort due to:

- changing systems or processes at entities
- staff shortages at entities resulting in poorer financial management, reporting and audit preparedness
- complexities and prior year issues which have resulted in an increase in management letter findings (financial audit and information systems audit), with some entities receiving modified opinions (qualifications and disclaimers)
- implementation of revised or new auditing/accounting standards.

As a result, our audit teams and senior staff are required to apply additional scrutiny to maintain audit quality and consistently report issues across the sector.

Increase in professional salaries and contract audit firm fees
Public sector salary adjustments are one factor affecting fee increases, but salaries paid by our approved contract audit firms to retain professional staff also play a significant role in increasing costs. Our approved contract audit firms have significantly increased their audit fees (average of 38% for local government entities). This is consistent with the prior year and reflective of the market, specifically for the auditing profession who, as with the OAG, are experiencing significant labour constraints and wage inflation. It also reflects the firms allowing enough hours to properly address the issues being encountered in many public sector finance functions.

The average fee increase across our audit portfolio of local government sector is 21%.

The specific reasons for the fee increase for your entity are:

- a large number of issues (i.e., management letter findings or technical issues) have previously been identified at the entity
- we have not been fully recovering our contract audit firm fee in recent years – in such instances we have adjusted to fully recover such and a reasonable proportion of our own time and costs.

How we can work together to minimise audit fees
We request that you submit certified financial report to our audit team at the commencement of the final visit. You will also need to provide key information and have staff available during the audit process. Being better prepared and audit ready should mean fewer queries from the audit team, which contributes to timely completion of the audit and potentially reduced costs.

We encourage your finance team to use the *Audit Readiness - Better Practice Guide*. This will help you maintain a sound control environment and provide timely and well-prepared financial report, working papers etc to our audit team. By being better prepared and audit-ready, our audit team is likely to have fewer queries, which contributes to timely completion and potentially reduced costs.

We will re-assess the costs for your audit closer to audit completion and inform you if a fee revision is necessary. A fee revision will only occur after we consult with you.

We look forward to working with you to promote accountability and transparency in the local government sector for the benefit of the community we jointly serve.

Please contact your Engagement Leader Aram Madnack on 6557 7674 if you require further information.

Yours sincerely

Aram Madnack
Acting Senior Director
Financial Audit
9 July 2024

YOUR AUDIT FEE - LOCAL GOVERNMENT

Opinion delivery year 2024-25

Band	Average fee	Median fee	Average increase	Average increase	Median increase	Median increase	Range
1	$116,690	$108,600	$14,290	15%	$12,910	10%	$79,000 - $198,702
2	$85,276	$94,600	$9,571	15%	$9,500	10%	$40,500 - $150,200
3	$56,890	$48,000	$8,935	21%	$8,410	21%	$29,000 - $108,350
4	$41,962	$39,500	$8,247	26%	$8,385	25%	$29,600 - $75,300
Regional Councils	$48,275	$32,850	$4,731	14%	$3,775	10%	$26,200 - $137,500

Cost to deliver opinions per LG opinion

Year	WA average	National average
2022-23	$62,750	$69,619
2023-24	$71,240	$91,252

OAG
Office of the Auditor General
Serving the Public Interest

5.3 PROGRESS UPDATE - AUDIT REPORTS	
LOCATION/ADDRESS:	Nil
APPLICANT:	Nil
FILE:	COA01
AUTHOR:	Project Officer
CONTRIBUTOR/S:	Manager Financial Services
RESPONSIBLE OFFICER:	Acting Director Corporate Services
DISCLOSURE OF INTEREST:	Nil

SUMMARY:

The Audit and Risk Committee are presented a progress update of the findings identified in the:

a) 2022/2023 Final Audit Management Report;
b) Interim Audit Management Report for year ended 30 June 2024; and
c) Performance Audit 2024 – Local Government Physical Security Server Room Assets (Emerging Findings).

BACKGROUND

2022/2023 Final Audit Management Report

SMC 21 December 2023	Item 5.4.1
ARC 22 April 2024	Item 6.2

The Shire's Final Audit Management Report for the 2022/2023 financial year was received by Council at the SMC 21 December 2023, in Confidential Attachment 3 of the Audit and Risk Committee Minutes of 19 December 2023.

An update of the progress of audit findings contained in the Shire's 2023 Final Audit Management Report was received by the Audit and Risk Committee at ARC 22 April 2024 and the following was resolved:

COMMITTEE RESOLUTION:

(REPORT RECOMMENDATION) Minute No. AR/0424/003

Moved: Shire President C Mitchell Seconded: Cr M Virgo That the Audit and Risk Committee recommends that Council:

1. Receive the progress update of findings as per Confidential Attachment 1; and

2. Requests the Chief Executive Officer to progress the finalisation of all outstanding findings as soon as practicable.

CARRIED UNANIMOUSLY 3/0

2023/2024 Interim Audit Management Report

The Shire's Interim Audit was conducted by RSM Australia (RSM) on behalf of the Office of the Auditor General (OAG) on 15-19 April 2024. A copy of the Interim Audit Management Report has been tabled in a separate item of this Audit Risk Committee meeting.

2024 Performance Audit – Local Government Physical Security of Server Room Assets (Emerging Findings)

A Performance Audit of 16 non-metropolitan local government entities was undertaken by the OAG to assess whether each local government effectively managed their physical server assets to protect them from physical and environmental hazards. Each local government received an Emerging Findings Letter which contained specific findings to the local government and a Summary of Findings Report which was tabled in State Parliament under sections 24 and 25 of the *Auditor General Act 2006.*

A copy of the Emerging Findings Letter and Summary of Findings Report has been tabled in a separate item of this Audit Risk Committee meeting.

COMMENT

A progress update of audit findings identified in:

a) 2022/2023 Final Audit Management Report;

b) 2023/2024 Interim Audit Management Report; and

c) 2024 Performance Audit – Local Government Physical Security Sever Room Assets (Emerging Findings),

is presented in ***Confidential Attachment 1*** for the Audit and Risk Committee to receive. Details contained within the report are considered confidential as releasing them publicly would increase the likelihood that identified risks could be the target of fraudulent or illegal activities.

Officers are actively addressing the issues highlighted in external audits. Each finding is categorised as completed, in progress, or overdue. Each audit finding is assigned a risk rating, facilitating the administration in prioritising and scheduling tasks for completion.

Efforts to manage overdue actions have been undertaken. Accountable Officers have provided updates regarding the tasks and progress to bring the actions to completion. In cases where feasible and reasonably foreseeable, new target completion dates are to be presented to OAG for mutual agreement.

A summary of the status of agreed management actions is found in the tables below:

OAG Audit Findings

Audit Type	Completed	In Progress – Not Due	Overdue	Total Findings
Final Audit 23/24	7	1	6	14
Interim Audit 23/24	2	4		6
2024 Performance Audit – Server Rooms	1	1		2
	10	**6**	**6**	**22**

CONSULTATION

Office of the Auditor General
RSM Australia

STATUTORY ENVIRONMENT

Local Government Act 1995

7.12A (3) Duties of local government with respect to audits

(3) A local government must —

(aa) examine an audit report received by the local government; and

(a) determine if any matters raised by the audit report, require action to be taken by the local government; and

(b) ensure that appropriate action is taken in respect of those matters

POLICY IMPLICATIONS

Nil.

FINANCIAL IMPLICATIONS

No specific financial implications are associated with this item. Remediation of any of the issues raised within the Audit Management Reports or Emerging Finding Letter may require budget allocations to resolve. Where this requires funding outside of the existing 2024/2025 adopted annual budget, Responsible Officers would request budget allocations either through the Shire's Finance and Costing Review process, or as part of the 2025/2026 annual budget process.

RISK

The audit findings provide management with recommendations particularly to strengthen internal controls and reduce the likelihood of certain risks. Delays in progressing and completing the audit findings can be unfavourable to the organisation, but are also weighed against other demands on Shire resources, and the costs to the community.

STRATEGIC ASPIRATIONS

Performance	**We will deliver excellent governance, service & value for everyone.**
Outcome 13	***Value for money from rates and long term financial sustainability***
Objective	13.1 Plan effectively for short- and long-term financial sustainability
Outcome 14	***Excellence in organisational performance and service delivery***
Objective	14.3 Monitor and continuously improve performance levels.

VOTING REQUIREMENTS
Simple Majority

REPORT RECOMMENDATION:

That the Audit and Risk Committee recommends that Council:

1. *Receive the progress update of findings as per* ***Confidential Attachment*** *1; and*
2. *Requests the Chief Executive Officer to progress the finalisation of all outstanding findings as soon as practicable.*

Attachments

1. Audit Progress Review Update *(Confidential to Councillors and Directors Only)*
   This attachment is confidential in accordance with section 5.23(2) of the Local Government Act 1995 section 5.23(2)((f)(ii)) as it contains "a matter that if disclosed, could be reasonably expected to endanger the security of the local governments property".

6. MEETING CLOSURE

These minutes were confirmed at a meeting held (DD Month Year),

and signed below by the Presiding Person, at the meeting these minutes were confirmed.

Signed: ……