CITY OF VINCENT

MINUTES

Audit and Risk Committee

26 February 2025

Table of Contents

MINUTES OF CITY OF VINCENT
AUDIT AND RISK COMMITTEE
HELD AT THE E-MEETING AND ADMINISTRATION AND CIVIC CENTRE
244 VINCENT STREET, LEEDERVILLE
ON WEDNESDAY, 26 FEBRUARY 2025 AT 4.15PM

PRESENT:	**Mr George Araj**	**Independent External Member (Chair)**
	Mr Conley Manifis	**Independent External Member**
	Mr Baptiste Isambert	**Independent External Member**
	Cr Alex Castle	**North Ward**
	Cr Jonathan Hallett	**South Ward (from 4.12pm)**
	Mayor Alison Xamon	**Presiding Member**
IN ATTENDANCE:	**David MacLennan**	**Chief Executive Officer**
	Rhys Taylor	**Executive Director Community & Business Services**
	Joslin Colli	**Executive Manager Corporate Strategy & Governance (from 4.09pm)**
	Emma Simmons	**Chief Audit Executive**
	Peter Ferguson	**Executive Manager Information & Communication Technology**
	Main Bhuiyan	**Manager Financial Services**
	Carrie Miller	**Corporate Strategy & Governance Officer**
	Prue Reddingius	**Manager Public Health & Built Environment (Item 5.4 only)**
	Cait McGowan	**OAG, Director Financial Audit (Item 6.1 only)**
	David Kilgren	**Office of the Auditor General (Item 6.1 only)**

1 INTRODUCTION AND WELCOME

The Presiding Member, George Araj, declared the meeting open at 4.09pm and read the following Acknowledgement of Country statement:

“The City of Vincent would like to acknowledge the Traditional Owners of the land, the Whadjuk people of the Noongar nation and pay our respects to Elders past, present and emerging”.

2 APOLOGIES / MEMBERS ON APPROVED LEAVE OF ABSENCE

Cr Ron Alexander

3 DECLARATIONS OF INTEREST

Conley Manifis declared an impartiality interest. The extent of his interest is that his company is contracted by the Office of the Auditor General to complete external audits.

4 CONFIRMATION OF MINUTES

COMMITTEE DECISION

Moved: Mr Manifis, Seconded: Mr Isambert

That the minutes of the Audit and Risk Committee held on 7 November 2024 be confirmed.

CARRIED (5-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

(Cr Hallett was absent from the Council Chamber and did not vote.)

As the Office of the Auditor General representatives were in attendance, the Presiding Member decided that this item would be moved to the first item of business for consideration.

At 4.12pm, Cr Jonathan Hallett arrived at the meeting during the OAG presentation.

6 GENERAL BUSINESS

6.2 OAG ENTRANCE MEETING 2024/25 AUDIT

Cait McGowan from the OAG presented the Audit Plan Summary for the City, highlighting no significant changes in processes, a reduction in on-site hours, and a focus on procurement and asset valuation.

6.1 OAG ENTRANCE MEETING 2024/25 AUDIT

Attachments: 1. Planning Summary - 30 June 2025 - Confidential

RECOMMENDATION:

That the Audit Committee recommends to Council that it NOTES the audit planning summary for the 2024/2025 financial year.

COMMITTEE DECISION ITEM 6.1

Moved: Mayor Xamon Seconded: Cr Castle,

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

At 4.21pm Cait McGowan and David Kilgren left the meeting and did not return.

At 4.22pm, the Manager Public Health & Built Environment arrived at the meeting prior to general business.

5 BUSINESS ARISING

As the Manager Public Health & Built Environment was in attendance to speak to Item 5.4, the Presiding Member decided that this item would be moved to the second item of business for consideration.

5.4 INTERNAL AUDIT REPORT (Y3 AUDIT 1) - SWIMMING POOL BARRIER INSPECTIONS

Attachments: 1. Swimming Pool Barrier Inspections Audit - Final - Confidential

RECOMMENDATION:

That the Audit Committee recommends to Council that it:

1. **RECEIVES the Swimming Pool Barrier Inspections Audit at Attachment 1;**

2. **NOTES the key findings of the review, as detailed in this report; and**

3. **NOTES that the findings and management actions arising from the review will be added to the City's Audit Log.**

COMMITTEE DECISION ITEM 5.4

Moved: Mayor Xamon, Seconded: Mr Manifis

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

5.1 OAG REPORTS ISSUED FOR LOCAL GOVERNMENT ENTITIES

Attachments:
1. **Local Government IT Disaster Recovery Planning** ⇩
2. **Local Government Management of Purchasing Cards** ⇩
3. **Local Government Physical Security of Server Assets** ⇩
4. **Staff Exit Controls at Large Local Government Entities** ⇩
5. **Better Practice Guide Supplier Master Files** ⇩

RECOMMENDATION:

That the Audit Committee RECEIVES:

1. **The reports from the Office of the Auditor General for the Local Government sector issued from May 2024 to June 2024; and**

2. **The Better Practice Guide: Supplier Master Files report from the Office of the Auditor General for all State and local government entities.**

COMMITTEE DECISION ITEM 5.1

Moved: Mayor Xamon, Seconded: Cr Hallett

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

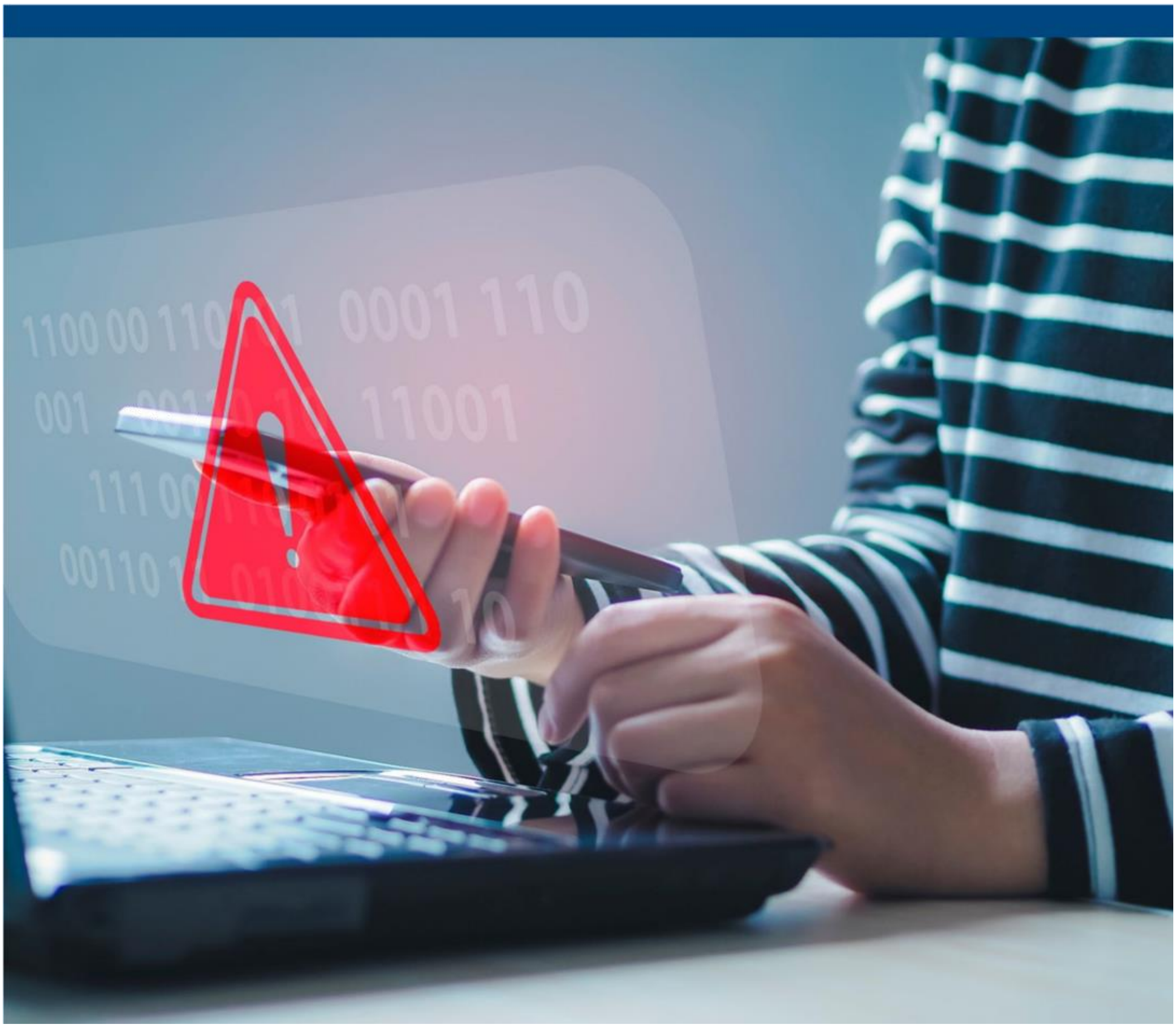
(Cr Alexander was an apology for the Meeting.)

OAG
Office of the Auditor General
Serving the Public Interest

Report 17: 2023-24 | 31 May 2024

PERFORMANCE AUDIT

Local Government IT Disaster Recovery Planning



Office of the Auditor General
for Western Australia

Audit team:
Aloha Morrissey
Paul Tilbrook
Adam Dias
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/Panya_photo

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government IT Disaster Recovery Planning

Report 17: 2023-24
31 May 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT IT DISASTER RECOVERY PLANNING

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

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

Caroline Spencer
Auditor General
31 May 2024

Contents

Auditor General's overview

Local government entities, like other public sector organisations, rely heavily on information technology (IT) systems to operate and deliver a vast range of services to their communities. This makes it increasingly important for all entities, regardless of their size, to have planned their response to disruptions such as cyber attacks and natural disasters.

My Office's previous information systems audits have consistently found issues with local government disaster recovery planning[1]. 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.

[1] Office of the Auditor General, *Local Government 2022-23 – Information Systems Audit Results*, OAG, 27 May 2024, accessed 28 May 2024.

Executive summary

Introduction

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

We have anonymised findings throughout this report to not compromise the security and continuity of systems and information at the entities. Detailed findings were provided to each entity.

Background

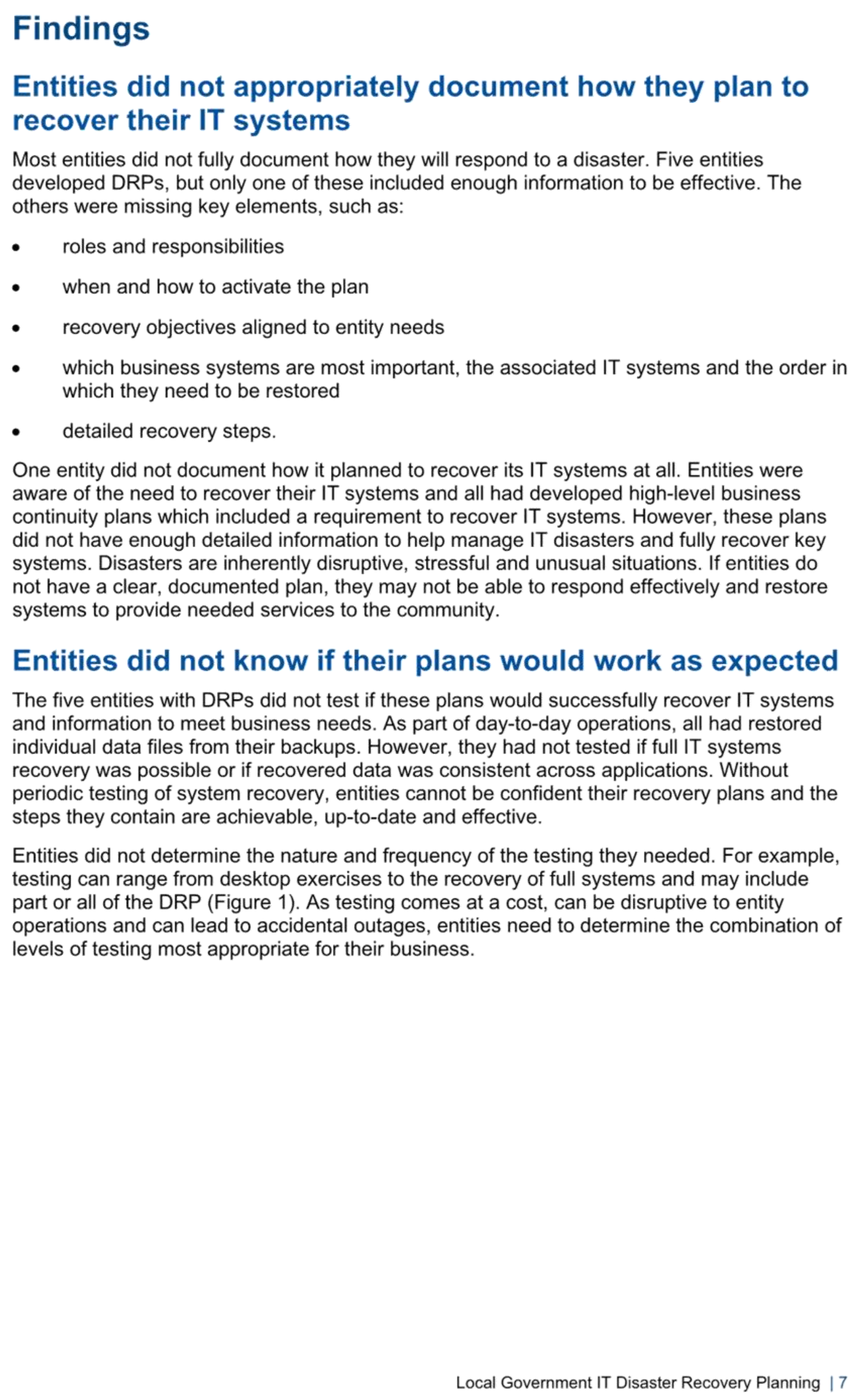
There are 147 local government entities in WA who provide key services and facilities to their communities. This may include waste management, road repair or broader services such as administration of marinas, cemeteries, airports, medical centres and retirement homes. All entities depend to some degree on functioning IT systems. These systems can be disrupted by disasters such as damage to equipment, cyber attacks, fire or flood. Any such disruption may impact an entity's ability to provide its services.

Entities can best prepare themselves to deal with the impact of a disaster on their systems through the process of IT disaster recovery planning. Good planning should consider several elements, including how and when the plan should be activated, who is responsible, and a clear description of recovery procedures (Appendix 1). These steps are typically captured in a disaster recovery plan (DRP). DRPs generally focus on major disruptions and are not concerned with minor issues such as system glitches or brief losses of communications that occur as part of normal day-to-day operations.

Conclusion

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. 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.



Findings

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. Five entities developed DRPs, but only one of these included enough information to be effective. The others were missing key elements, such as:

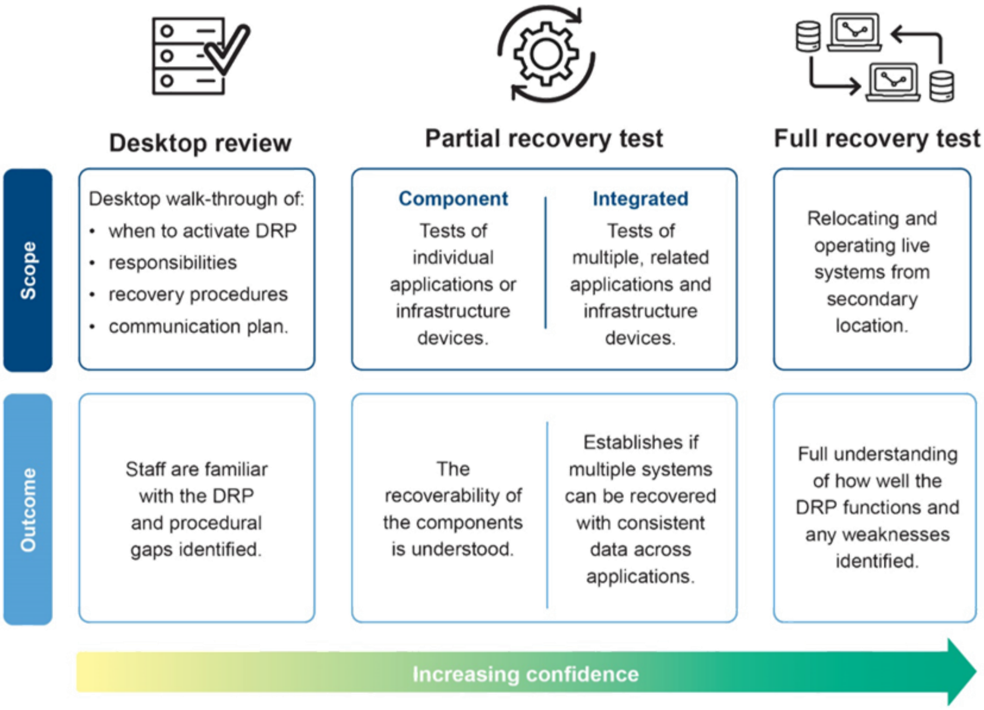
- roles and responsibilities
- when and how to activate the plan
- recovery objectives aligned to entity needs
- which business systems are most important, the associated IT systems and the order in which they need to be restored
- detailed recovery steps.

One entity did not document how it planned to recover its IT systems at all. Entities were aware of the need to recover their IT systems and all had developed high-level business continuity plans which included a requirement to recover IT systems. However, these plans did not have enough detailed information to help manage IT disasters and fully recover key systems. Disasters are inherently disruptive, stressful and unusual situations. If entities do not have a clear, documented plan, they may not be able to respond effectively and restore systems to provide needed services to the community.

Entities did not know if their plans would work as expected

The five entities with DRPs did not test if these plans would successfully recover IT systems and information to meet business needs. As part of day-to-day operations, all had restored individual data files from their backups. However, they had not tested if full IT systems recovery was possible or if recovered data was consistent across applications. Without periodic testing of system recovery, entities cannot be confident their recovery plans and the steps they contain are achievable, up-to-date and effective.

Entities did not determine the nature and frequency of the testing they needed. For example, testing can range from desktop exercises to the recovery of full systems and may include part or all of the DRP (Figure 1). As testing comes at a cost, can be disruptive to entity operations and can lead to accidental outages, entities need to determine the combination of levels of testing most appropriate for their business.



	Desktop review	Partial recovery test		Full recovery test
		Component	Integrated	
Scope	Desktop walk-through of: • when to activate DRP • responsibilities • recovery procedures • communication plan.	Tests of individual applications or infrastructure devices.	Tests of multiple, related applications and infrastructure devices.	Relocating and operating live systems from secondary location.
Outcome	Staff are familiar with the DRP and procedural gaps identified.	The recoverability of the components is understood.	Establishes if multiple systems can be recovered with consistent data across applications.	Full understanding of how well the DRP functions and any weaknesses identified.

Source: OAG based on ISO/IEC 27031:2011[2]

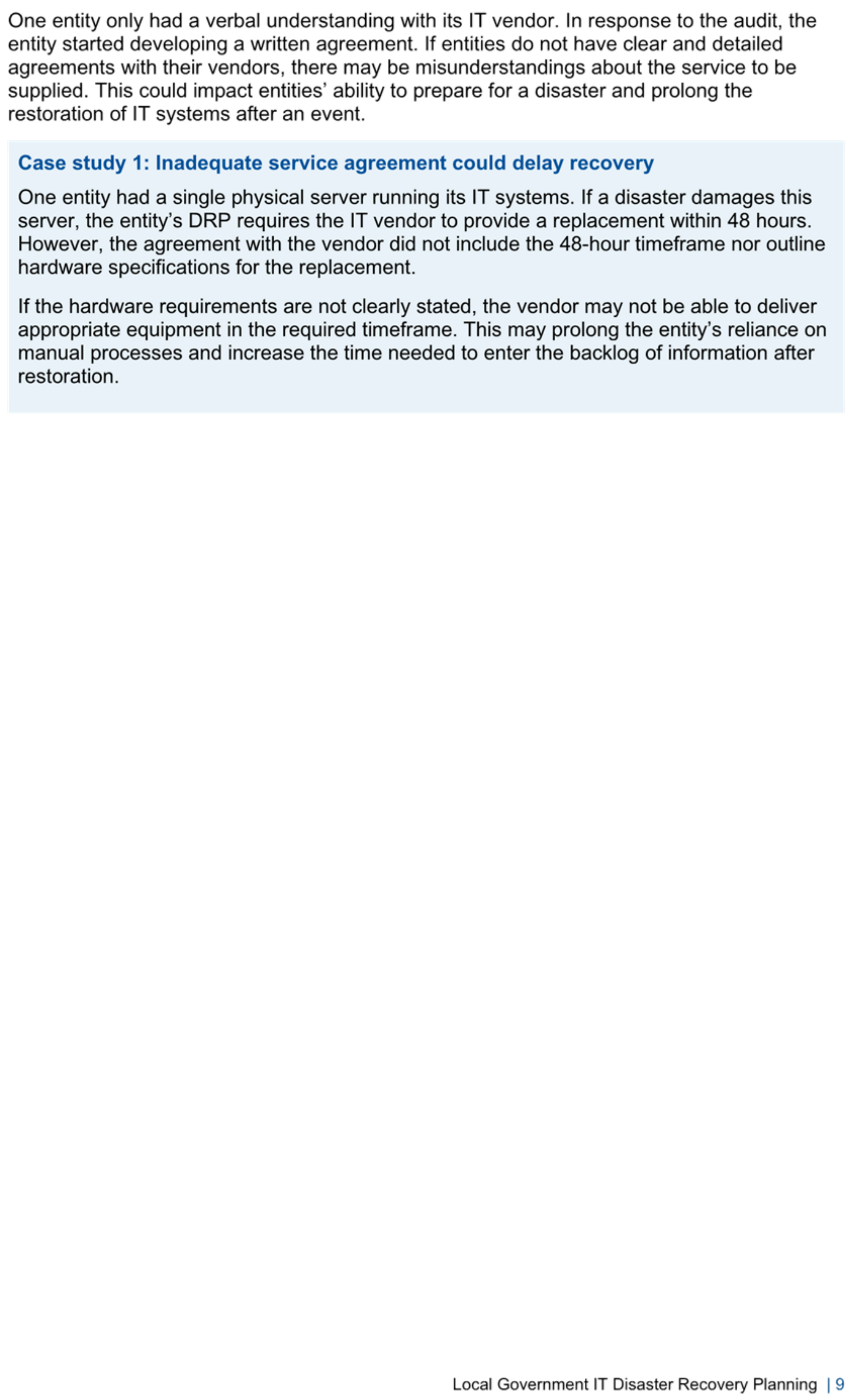
Figure 1: Levels of disaster recovery testing

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. Five had service agreements in place but these were missing all or some of the following:

- a clear description of the disaster recovery service required
- where the disaster recovery services are to be provided
- a description of the hardware required and delivery timeframes
- a clear requirement for the vendor to participate in disaster recovery planning
- how vendors are involved in testing (nature and frequency)
- timeframes for recovering from a disaster
- processes for monitoring, tracking and evaluating vendor performance
- recourse if expectations are not met.

[2] International Organization for Standardization and the International Electrotechnical Commission, *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*, ISO, 2011.

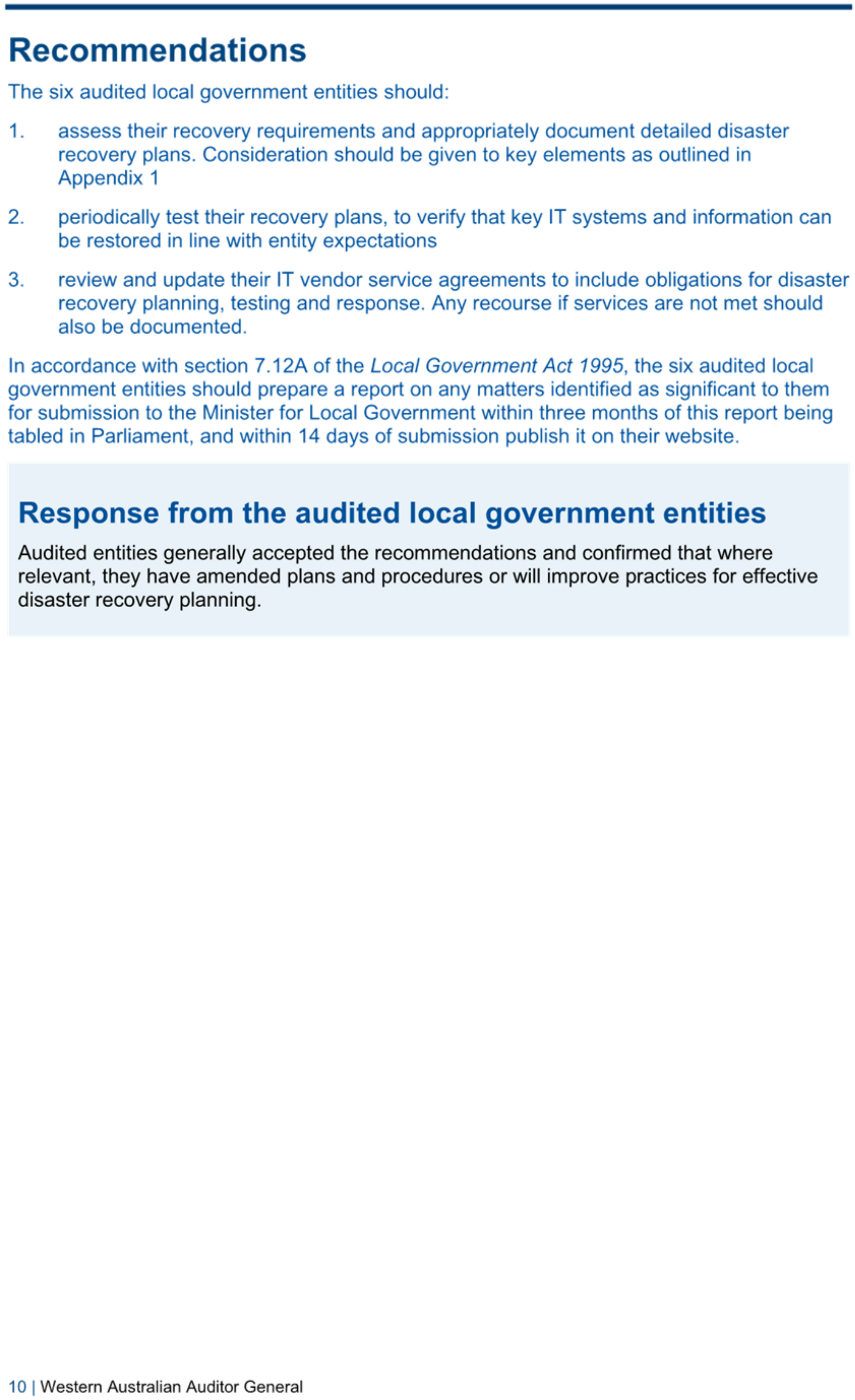


One entity only had a verbal understanding with its IT vendor. In response to the audit, the entity started developing a written agreement. If entities do not have clear and detailed agreements with their vendors, there may be misunderstandings about the service to be supplied. This could impact entities' ability to prepare for a disaster and prolong the restoration of IT systems after an event.

Case study 1: Inadequate service agreement could delay recovery

One entity had a single physical server running its IT systems. If a disaster damages this server, the entity's DRP requires the IT vendor to provide a replacement within 48 hours. However, the agreement with the vendor did not include the 48-hour timeframe nor outline hardware specifications for the replacement.

If the hardware requirements are not clearly stated, the vendor may not be able to deliver appropriate equipment in the required timeframe. This may prolong the entity's reliance on manual processes and increase the time needed to enter the backlog of information after restoration.



Recommendations

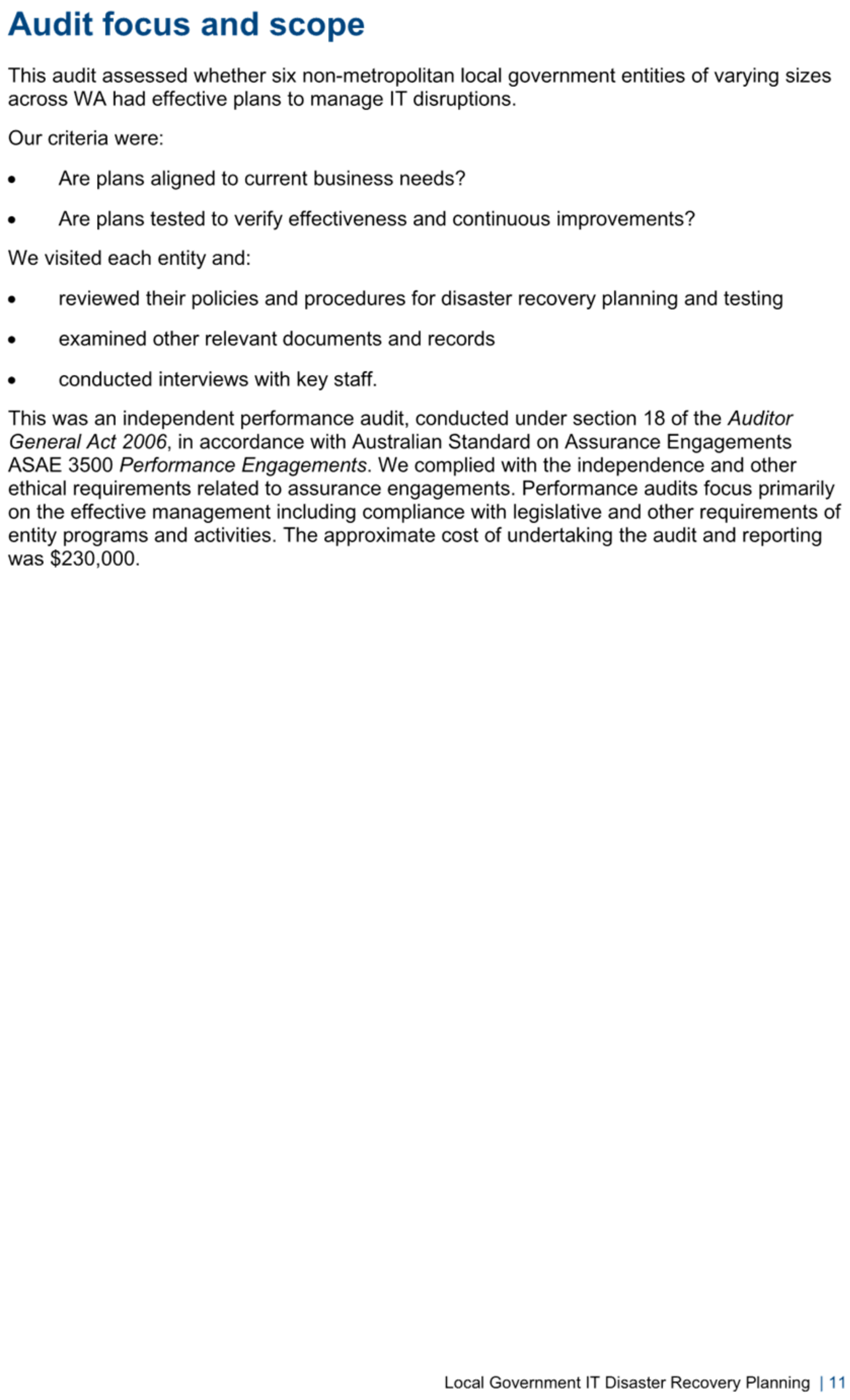
The six audited local government entities should:

1. assess their recovery requirements and appropriately document detailed disaster recovery plans. Consideration should be given to key elements as outlined in Appendix 1
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.

In accordance with section 7.12A of the *Local Government Act 1995*, the six 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 local government entities

Audited entities generally accepted the recommendations and confirmed that where relevant, they have amended plans and procedures or will improve practices for effective disaster recovery planning.



Audit focus and scope

This audit assessed whether six non-metropolitan local government entities of varying sizes across WA had effective plans to manage IT disruptions.

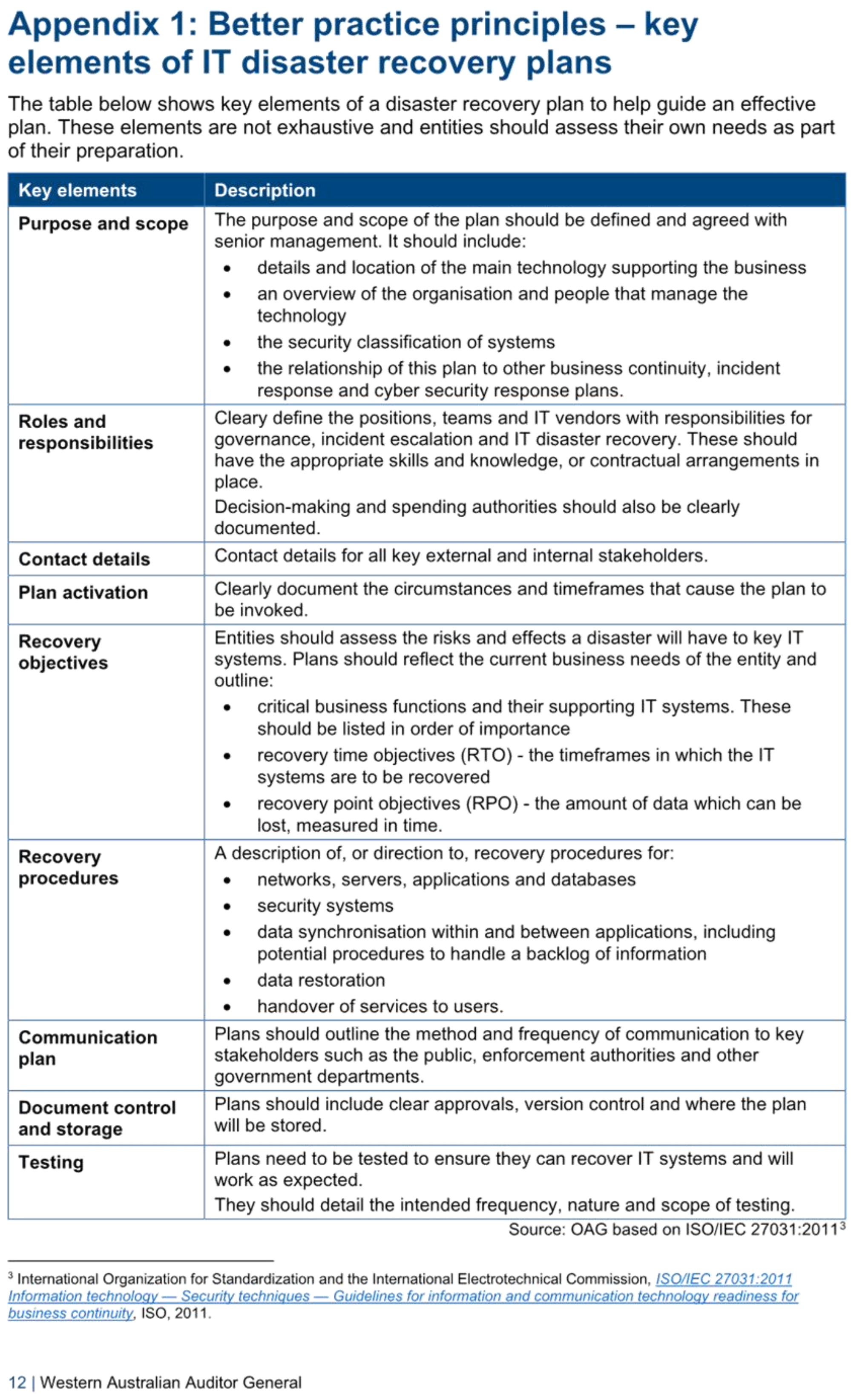
Our criteria were:

- Are plans aligned to current business needs?
- Are plans tested to verify effectiveness and continuous improvements?

We visited each entity and:

- reviewed their policies and procedures for disaster recovery planning and testing
- examined other relevant documents and records
- conducted interviews with key staff.

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 including compliance with legislative and other requirements of entity programs and activities. The approximate cost of undertaking the audit and reporting was $230,000.



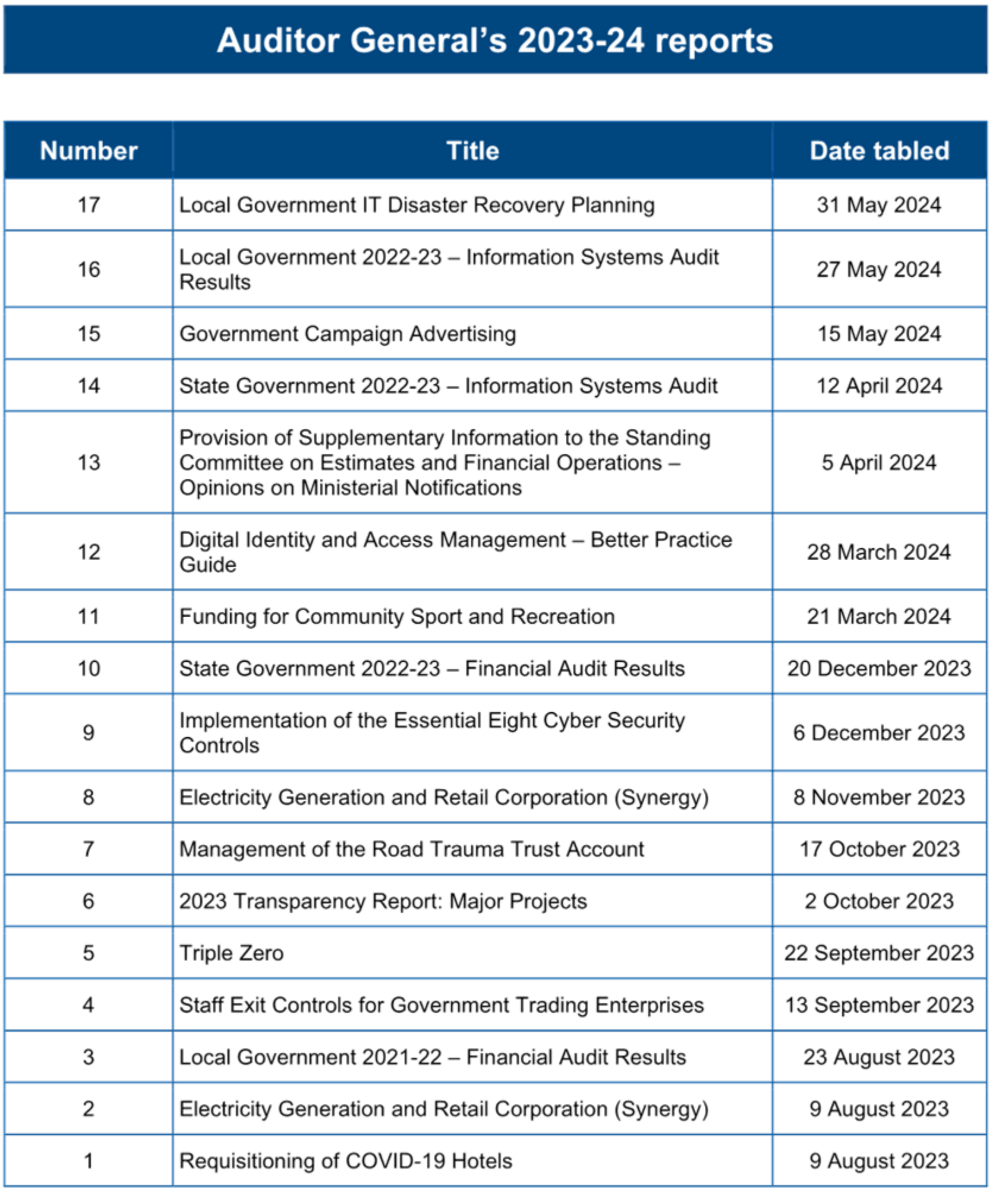
Appendix 1: Better practice principles – key elements of IT disaster recovery plans

The table below shows key elements of a disaster recovery plan to help guide an effective plan. These elements are not exhaustive and entities should assess their own needs as part of their preparation.

Key elements	Description
Purpose and scope	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.
Roles and responsibilities	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.
Contact details	Contact details for all key external and internal stakeholders.
Plan activation	Clearly document the circumstances and timeframes that cause the plan to be invoked.
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.
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 • data restoration • handover of services to users.
Communication plan	Plans should outline the method and frequency of communication to key stakeholders such as the public, enforcement authorities and other government departments.
Document control and storage	Plans should include clear approvals, version control and where the plan will be stored.
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.

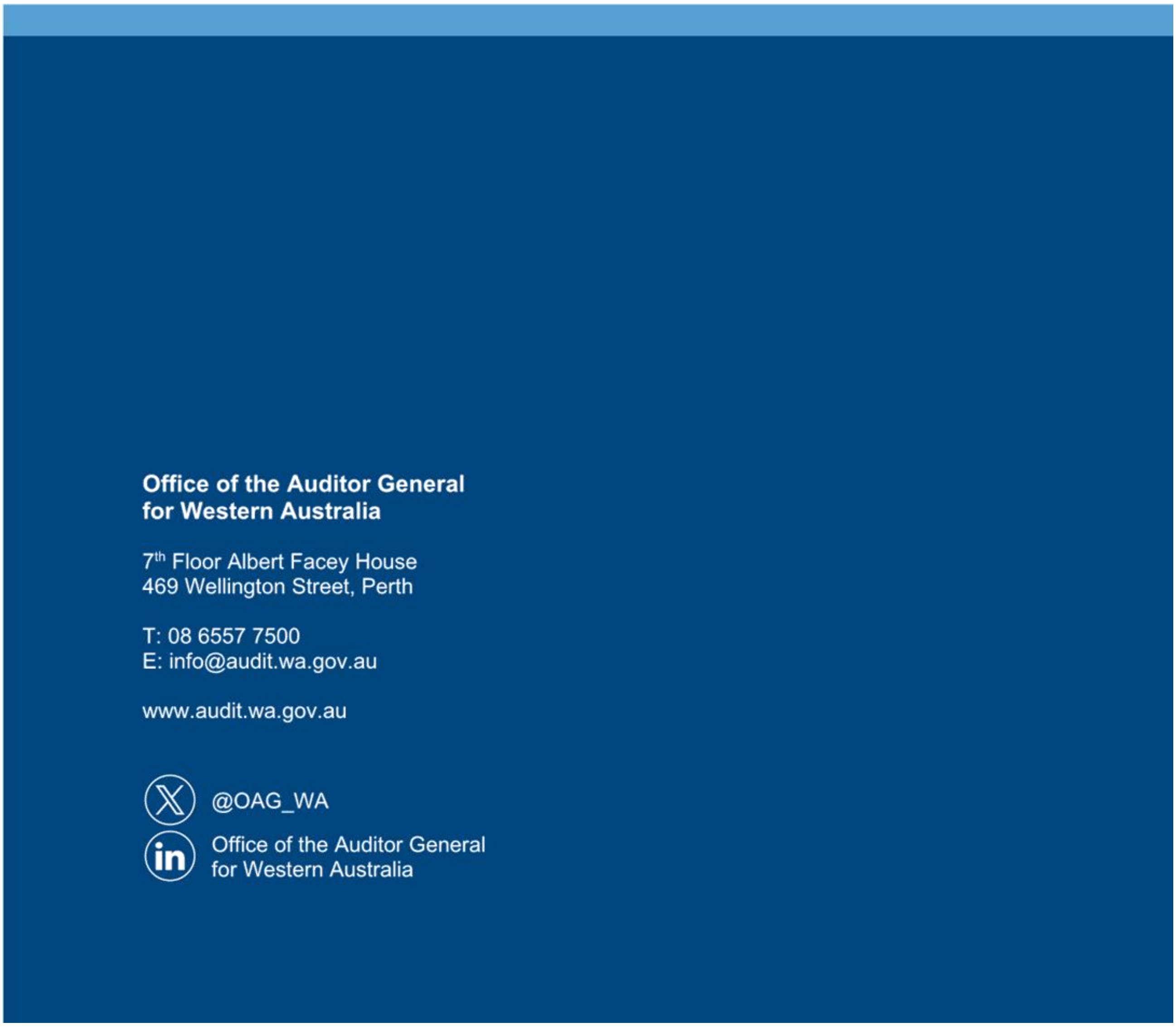
Source: OAG based on ISO/IEC 27031:2011[3]

[3] International Organization for Standardization and the International Electrotechnical Commission, *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*, ISO, 2011.



Auditor General’s 2023-24 reports

Number	Title	Date tabled
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
for 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

OAG
Office of the Auditor General
Serving the Public Interest

Report 19: 2023-24 | 12 June 2024

PERFORMANCE AUDIT

Local Government Management of Purchasing Cards

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Justine Mezzatesta
Claire Lieb
Dan Franks

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/Suradech Prapairat

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government Management of Purchasing Cards

Report 19: 2023-24
12 June 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT MANAGEMENT OF PURCHASING CARDS

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 three regional local government entities effectively managed the issue, use and cancellation of purchasing cards.

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

Caroline Spencer
Auditor General
12 June 2024

Contents

Auditor General's overview

Purchasing cards offer benefits for local government entities by streamlining purchasing activities. However, these benefits come with the risk of misuse and loss of public money if the purchasing cards are not effectively managed.

In this audit, we looked at the management of purchasing cards at three regional entities. While we found poor management of some important controls, we did not find clear evidence that cardholders misused public money, in part because the entities did not have policy guidance to underpin allowable and reasonable use.

This audit follows on from our 2018 audit of local government entities' use of credit cards[1], which found generally satisfactory controls but noted shortcomings of varying significance in policies and procedures. In addition, our *Local Government 2021-22 - Financial Audit Results*[2] report found 20 entities with credit card anomalies.

For a more comprehensive review of purchasing cards, this audit looked beyond the use of credit cards and included other cards such as store cards. In reviewing each entity's controls, we did not apply a 'one size fits all' approach as the diversity of the sector means some very small entities, with few cardholders, may not need the same controls as larger entities with more cardholders.

I encourage the sector to use our better practice guidance in Appendix 1 - it contains considerations to help mitigate the risks associated with the use of purchasing cards and for creating an effective control environment.

I thank the staff at each audited entity for their cooperation and assistance in completing this work, and strongly encourage all local government entities to assess their own policies and management of purchasing cards against the focus areas of this audit.

[1] Office of the Auditor General, *Controls Over Corporate Credit Cards*, OAG website, 9 May 2018.

[2] Office of the Auditor General, *Local Government 2021-22 Financial Audit Results*, OAG website, 23 August 2023.

Executive summary

Introduction

The audit assessed whether three regional local government entities (City of Albany, City of Kalgoorlie-Boulder and Shire of Murchison) effectively managed the issue, use and cancellation of purchasing cards. We last audited this topic in the local government sector in 2018[3].

In conducting the audit, we considered the requirements of the *Local Government Act 1995* (LG Act) and associated regulations, guidelines issued by the Department of Local Government, Sport and Cultural Industries (DLGSC) and our better practice guidance in Appendix 1.

Background

Purchasing cards represent an approved line of credit and are a well-established part of modern purchasing systems. They include corporate credit cards, store cards[4], fuel cards and taxi cards. These cards provide entities with a cost effective, convenient and timely way to pay for goods and services of low value.

Local government entities need to have effective controls, appropriate to their size and risk, to prevent and detect inadvertent or deliberate misuse of their purchasing cards and meet their legislated responsibilities around the allocation of finances. This includes being able to demonstrate that purchases meet a business need and meet the expectations of ratepayers in the responsible use of public money. Improper, wasteful or unauthorised purchases that are not identified and resolved can result in financial loss to the entity.

The *Local Government Act 1995* (LG Act) and associated regulations require:

- entities to develop procedures for the payment of accounts to ensure there is effective security for, and properly authorised use of purchasing cards[5].
- the CEO to keep proper accounts and records in accordance with regulations[6]
- the council to oversee allocation of the local government's finances and resources and determine policies[7]
- entities to provide information about each purchasing card transaction in a payment listing to council and in council minutes to increase transparency, accountability and council oversight of incidental spending[8].

An effective control environment for purchasing cards should include:

- controls to prevent misuse and errors. These controls establish requirements up-front, and before a purchase is made. Examples include clear policies and procedures,

[3] Office of the Auditor General, Controls Over Corporate Credit Cards, OAG website, 9 May 2018.

[4] Australian Securities and Investments Commission, store card, Moneysmart.gov.au, n.d., accessed 29 April 2024.

[5] Local Governments (Financial Management) Regulations 1996, regulation 11(1)a.

[6] *Local Government Act 1995* section 6.5(a).

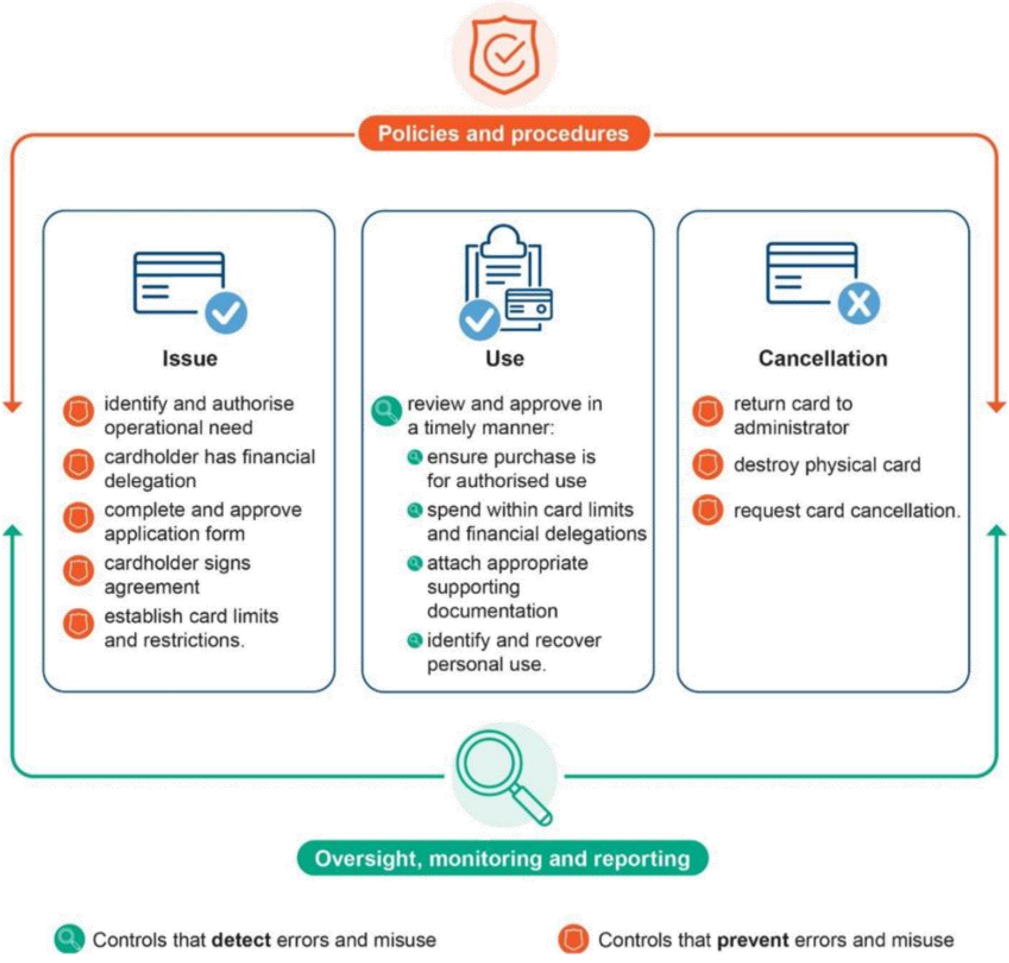
[7] *Local Government Act 1995* sections 2.7(2)(a) and (b).

[8] Local Government (Financial Management) Regulations 1996, regulation 13A took effect from 1 September 2023.

delegations to purchase, preset card limits and appropriate card authorisation and destruction processes.

- controls to detect errors and misuse after a purchase is made. These include processes to review and approve purchases, and the monitoring, reporting and oversight of card use.

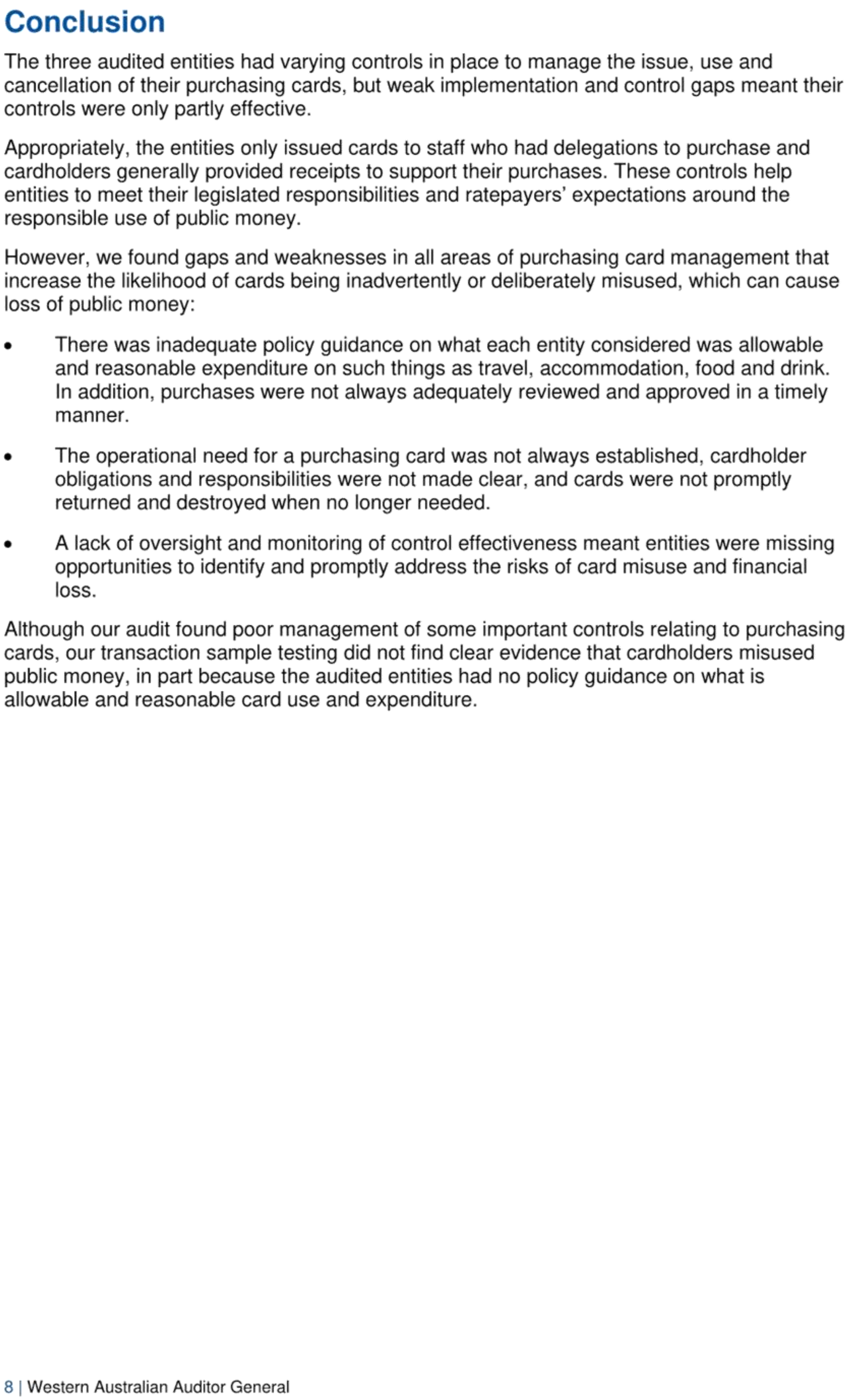
Figure 1 provides an overview of the key components of purchasing card management, highlighting the controls we assessed during the audit and our better practice guidance (Appendix 1).


Policies and procedures
Issue
identify and authorise operational need
cardholder has financial delegation
complete and approve application form
cardholder signs agreement
establish card limits and restrictions.
Use
review and approve in a timely manner:
ensure purchase is for authorised use
spend within card limits and financial delegations
attach appropriate supporting documentation
identify and recover personal use.
Cancellation
return card to administrator
destroy physical card
request card cancellation.
Oversight, monitoring and reporting
Controls that **detect** errors and misuse
Controls that **prevent** errors and misuse

Source: OAG

Figure 1: Overview of the key components in purchasing card management and controls

The DLGSC provides the sector with broad guidance on the management of purchasing cards and changes in legislation through accounting and operational guidelines, circulars, alert bulletins and monthly webinars.



Conclusion

The three audited entities had varying controls in place to manage the issue, use and cancellation of their purchasing cards, but weak implementation and control gaps meant their controls were only partly effective.

Appropriately, the entities only issued cards to staff who had delegations to purchase and cardholders generally provided receipts to support their purchases. These controls help entities to meet their legislated responsibilities and ratepayers' expectations around the responsible use of public money.

However, we found gaps and weaknesses in all areas of purchasing card management that increase the likelihood of cards being inadvertently or deliberately misused, which can cause loss of public money:

- There was inadequate policy guidance on what each entity considered was allowable and reasonable expenditure on such things as travel, accommodation, food and drink. In addition, purchases were not always adequately reviewed and approved in a timely manner.
- The operational need for a purchasing card was not always established, cardholder obligations and responsibilities were not made clear, and cards were not promptly returned and destroyed when no longer needed.
- A lack of oversight and monitoring of control effectiveness meant entities were missing opportunities to identify and promptly address the risks of card misuse and financial loss.

Although our audit found poor management of some important controls relating to purchasing cards, our transaction sample testing did not find clear evidence that cardholders misused public money, in part because the audited entities had no policy guidance on what is allowable and reasonable card use and expenditure.

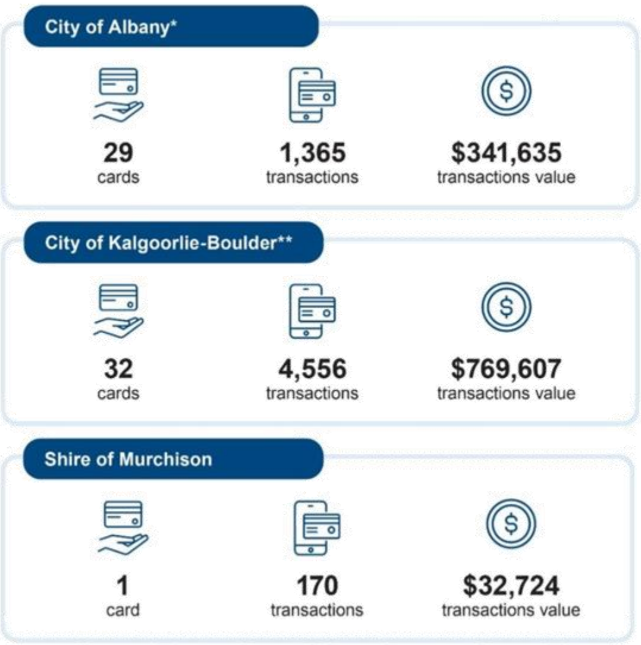
Findings

Controls over the use of purchasing cards were partly effective

We found cardholders generally provided receipts for their purchases and had appropriate delegations to purchase. However, we identified control weaknesses of varying significance across the three audited entities which increased the likelihood of unreasonable or unauthorised purchases. Detailed findings were provided to each of the audited entities.

Entities need to develop clear policy guidance on what is allowable and reasonable business expenditure, regardless of the payment mechanism, and improve card expenditure review and approval processes to prevent and detect inadvertent or deliberate misuse.

The three entities varied in the number of cards issued and the number of purchases over the audit period (Figure 2). All were using their purchasing cards to make low value purchases with most transactions being for items less than $500.



Source: OAG based on information provided by each entity

** City of Albany: 5 credit cards (1,018 transactions and $318,543) and 24 store cards (347 transactions and $23,092).*

*** City of Kalgoorlie-Boulder: 30 credit cards (4,434 transactions and $759,181) and 2 store cards (122 transactions and $10,426).*

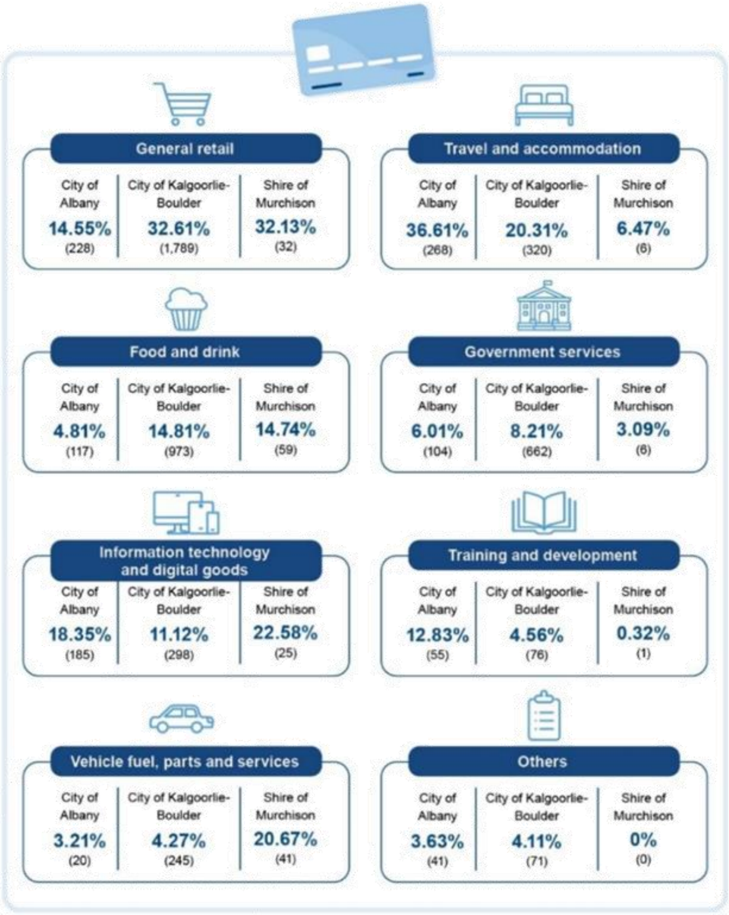
Figure 2: Key purchasing card statistics for 1 November 2022 to 31 December 2023

Our analysis found card purchases generally fell into the following categories:

- general retail (e.g. industrial and construction supplies, hardware and equipment, and office supplies and printing)

- travel and accommodation
- food and drink purchases
- government services (e.g. postal services, licenses, registrations and permits)
- information technology and digital goods
- training and development
- vehicle fuel, parts and services
- others.

We further analysed credit card purchases, which made up most of the purchases over the audit period.[9] Figure 3 shows the percentage spend and the number of purchases in each category by entity.

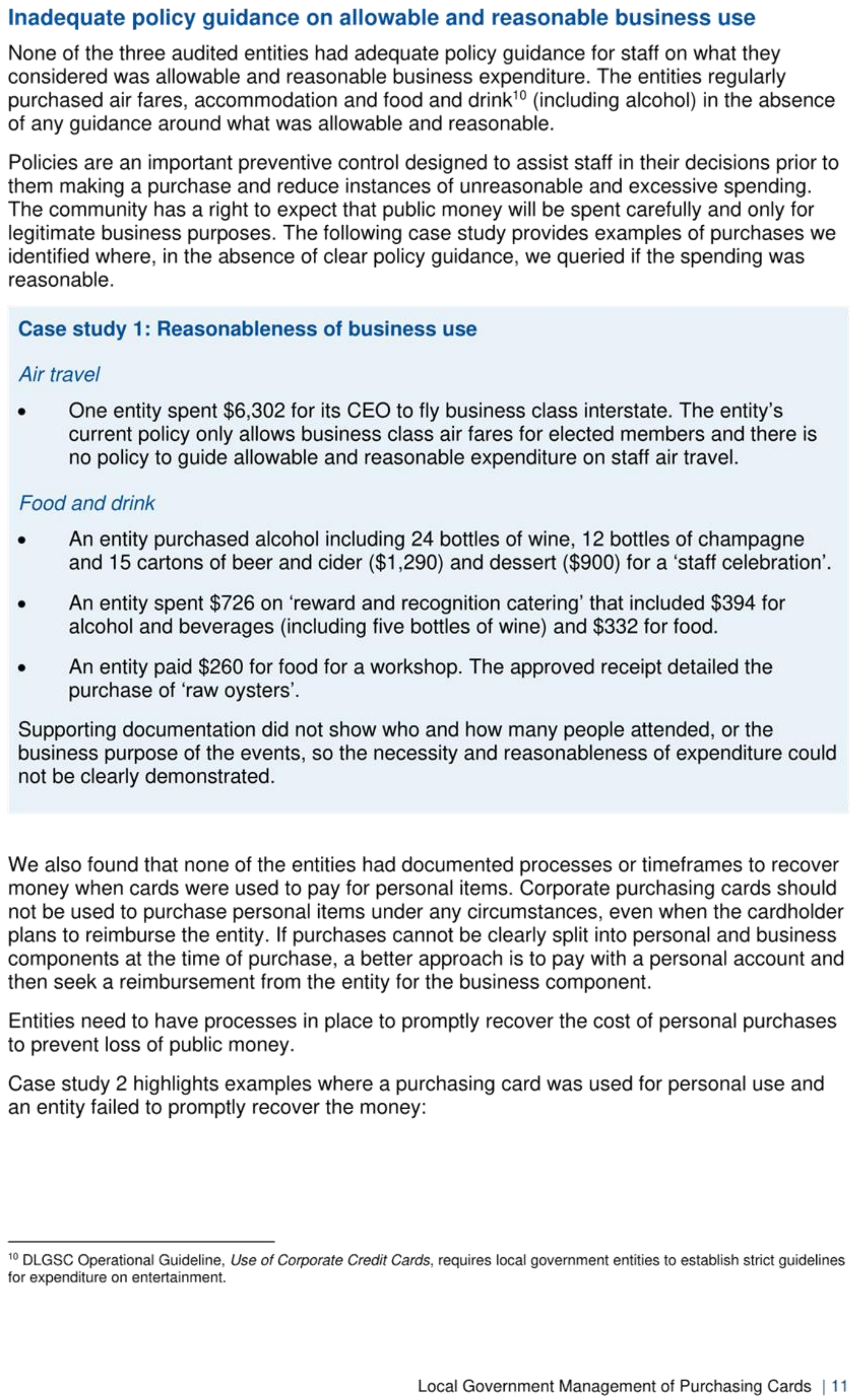


	City of Albany	City of Kalgoorlie-Boulder	Shire of Murchison
General retail	14.55% (228)	32.61% (1,789)	32.13% (32)
Travel and accommodation	36.61% (268)	20.31% (320)	6.47% (6)
Food and drink	4.81% (117)	14.81% (973)	14.74% (59)
Government services	6.01% (104)	8.21% (662)	3.09% (6)
Information technology and digital goods	18.35% (185)	11.12% (298)	22.58% (25)
Training and development	12.83% (55)	4.56% (76)	0.32% (1)
Vehicle fuel, parts and services	3.21% (20)	4.27% (245)	20.67% (41)
Others	3.63% (41)	4.11% (71)	0% (0)

Source: OAG based on credit card information provided by each entity

Figure 3: Purchase categories for 1 November 2022 to 31 December 2023

[9] Credit card purchases were allocated using standard merchant information. Store card purchases were not analysed as merchant categories were not readily available.



Inadequate policy guidance on allowable and reasonable business use

None of the three audited entities had adequate policy guidance for staff on what they considered was allowable and reasonable business expenditure. The entities regularly purchased air fares, accommodation and food and drink[10] (including alcohol) in the absence of any guidance around what was allowable and reasonable.

Policies are an important preventive control designed to assist staff in their decisions prior to them making a purchase and reduce instances of unreasonable and excessive spending. The community has a right to expect that public money will be spent carefully and only for legitimate business purposes. The following case study provides examples of purchases we identified where, in the absence of clear policy guidance, we queried if the spending was reasonable.

Case study 1: Reasonableness of business use

Air travel

- One entity spent $6,302 for its CEO to fly business class interstate. The entity's current policy only allows business class air fares for elected members and there is no policy to guide allowable and reasonable expenditure on staff air travel.

Food and drink

- An entity purchased alcohol including 24 bottles of wine, 12 bottles of champagne and 15 cartons of beer and cider ($1,290) and dessert ($900) for a 'staff celebration'.
- An entity spent $726 on 'reward and recognition catering' that included $394 for alcohol and beverages (including five bottles of wine) and $332 for food.
- An entity paid $260 for food for a workshop. The approved receipt detailed the purchase of 'raw oysters'.

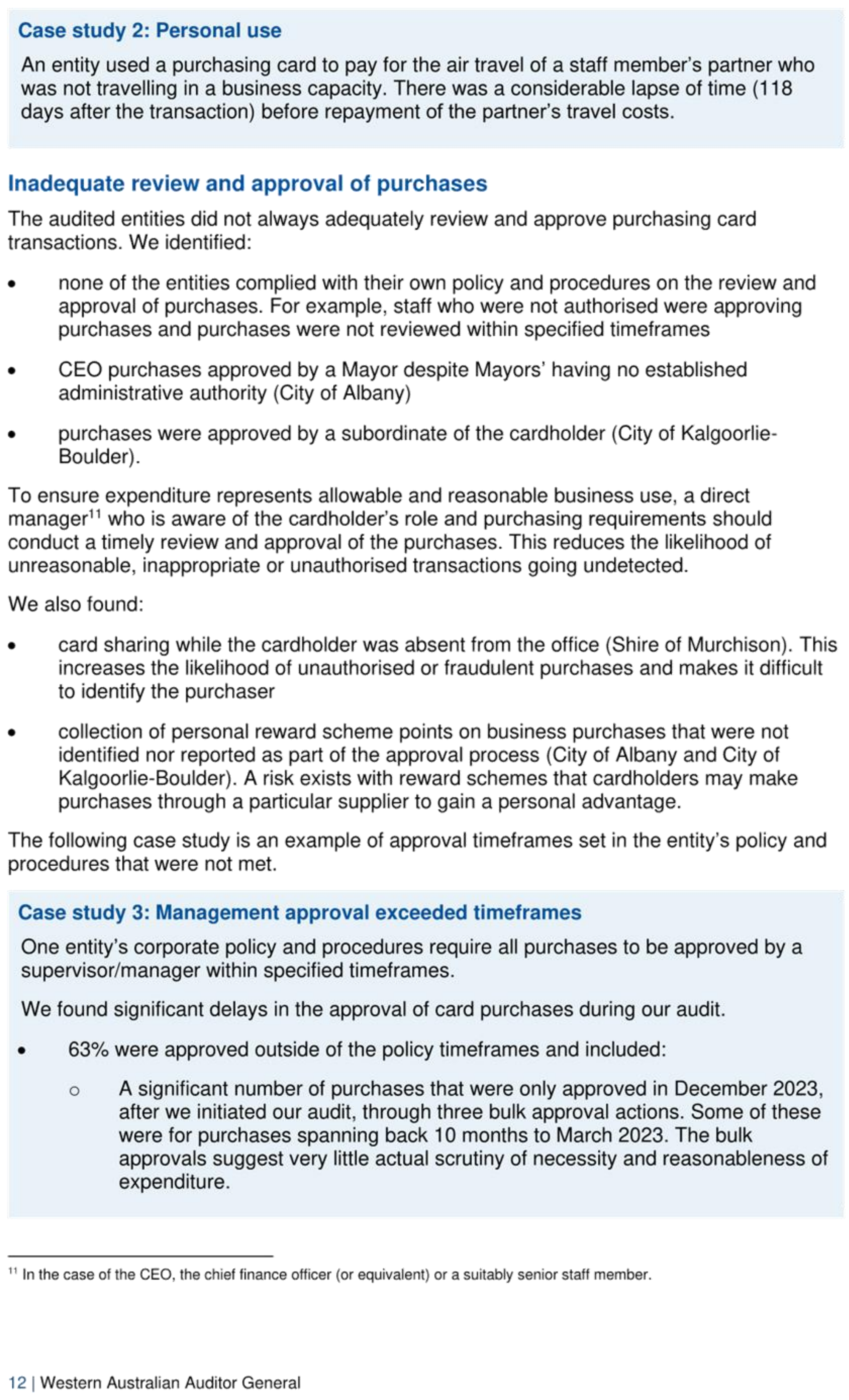
Supporting documentation did not show who and how many people attended, or the business purpose of the events, so the necessity and reasonableness of expenditure could not be clearly demonstrated.

We also found that none of the entities had documented processes or timeframes to recover money when cards were used to pay for personal items. Corporate purchasing cards should not be used to purchase personal items under any circumstances, even when the cardholder plans to reimburse the entity. If purchases cannot be clearly split into personal and business components at the time of purchase, a better approach is to pay with a personal account and then seek a reimbursement from the entity for the business component.

Entities need to have processes in place to promptly recover the cost of personal purchases to prevent loss of public money.

Case study 2 highlights examples where a purchasing card was used for personal use and an entity failed to promptly recover the money:

[10] DLGSC Operational Guideline, *Use of Corporate Credit Cards*, requires local government entities to establish strict guidelines for expenditure on entertainment.



Case study 2: Personal use

An entity used a purchasing card to pay for the air travel of a staff member's partner who was not travelling in a business capacity. There was a considerable lapse of time (118 days after the transaction) before repayment of the partner's travel costs.

Inadequate review and approval of purchases

The audited entities did not always adequately review and approve purchasing card transactions. We identified:

- none of the entities complied with their own policy and procedures on the review and approval of purchases. For example, staff who were not authorised were approving purchases and purchases were not reviewed within specified timeframes
- CEO purchases approved by a Mayor despite Mayors' having no established administrative authority (City of Albany)
- purchases were approved by a subordinate of the cardholder (City of Kalgoorlie-Boulder).

To ensure expenditure represents allowable and reasonable business use, a direct manager[11] who is aware of the cardholder's role and purchasing requirements should conduct a timely review and approval of the purchases. This reduces the likelihood of unreasonable, inappropriate or unauthorised transactions going undetected.

We also found:

- card sharing while the cardholder was absent from the office (Shire of Murchison). This increases the likelihood of unauthorised or fraudulent purchases and makes it difficult to identify the purchaser
- collection of personal reward scheme points on business purchases that were not identified nor reported as part of the approval process (City of Albany and City of Kalgoorlie-Boulder). A risk exists with reward schemes that cardholders may make purchases through a particular supplier to gain a personal advantage.

The following case study is an example of approval timeframes set in the entity's policy and procedures that were not met.

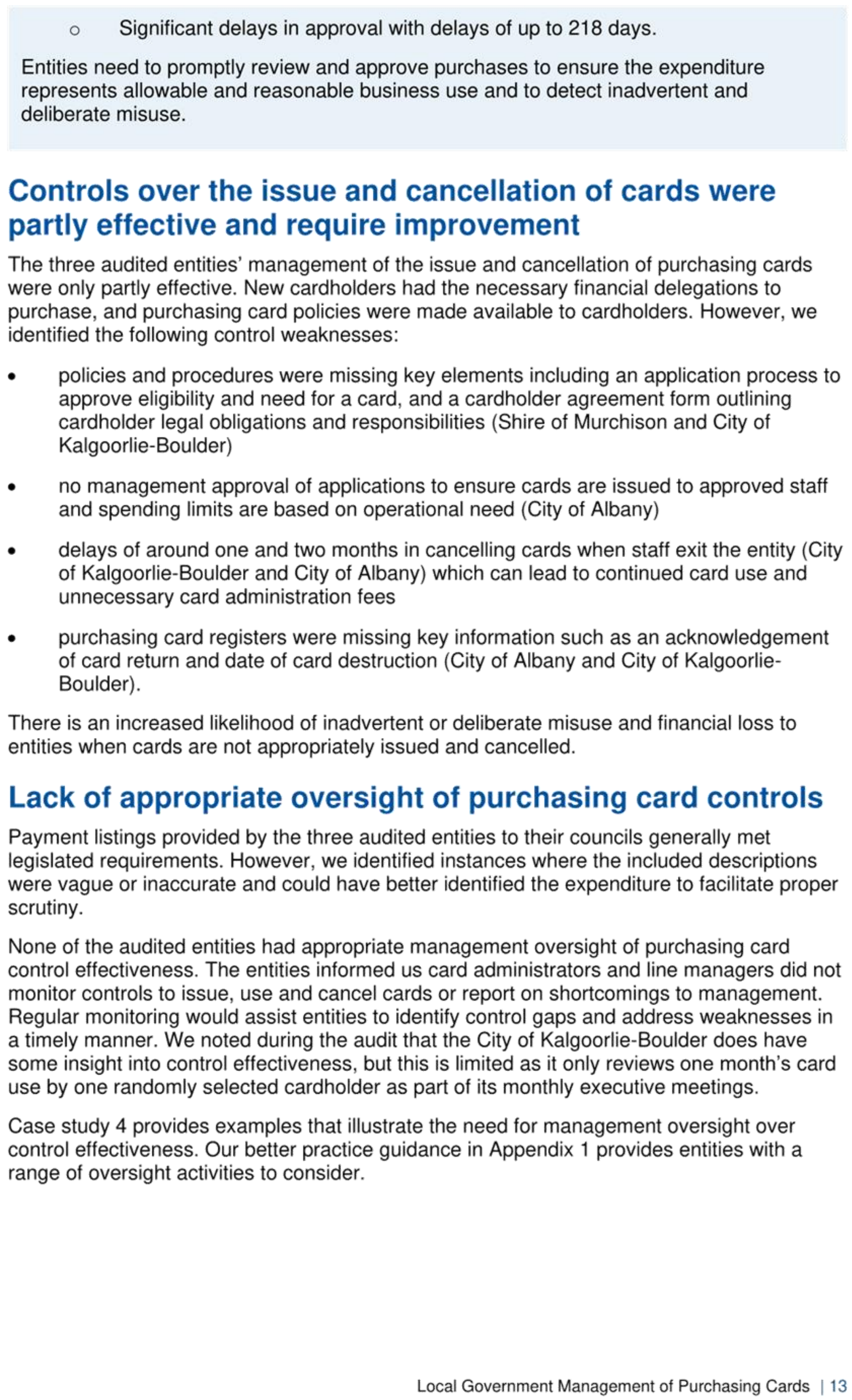
Case study 3: Management approval exceeded timeframes

One entity's corporate policy and procedures require all purchases to be approved by a supervisor/manager within specified timeframes.

We found significant delays in the approval of card purchases during our audit.

- 63% were approved outside of the policy timeframes and included:
  - A significant number of purchases that were only approved in December 2023, after we initiated our audit, through three bulk approval actions. Some of these were for purchases spanning back 10 months to March 2023. The bulk approvals suggest very little actual scrutiny of necessity and reasonableness of expenditure.

[11] In the case of the CEO, the chief finance officer (or equivalent) or a suitably senior staff member.



- Significant delays in approval with delays of up to 218 days.

Entities need to promptly review and approve purchases to ensure the expenditure represents allowable and reasonable business use and to detect inadvertent and deliberate misuse.

Controls over the issue and cancellation of cards were partly effective and require improvement

The three audited entities' management of the issue and cancellation of purchasing cards were only partly effective. New cardholders had the necessary financial delegations to purchase, and purchasing card policies were made available to cardholders. However, we identified the following control weaknesses:

- policies and procedures were missing key elements including an application process to approve eligibility and need for a card, and a cardholder agreement form outlining cardholder legal obligations and responsibilities (Shire of Murchison and City of Kalgoorlie-Boulder)
- no management approval of applications to ensure cards are issued to approved staff and spending limits are based on operational need (City of Albany)
- delays of around one and two months in cancelling cards when staff exit the entity (City of Kalgoorlie-Boulder and City of Albany) which can lead to continued card use and unnecessary card administration fees
- purchasing card registers were missing key information such as an acknowledgement of card return and date of card destruction (City of Albany and City of Kalgoorlie-Boulder).

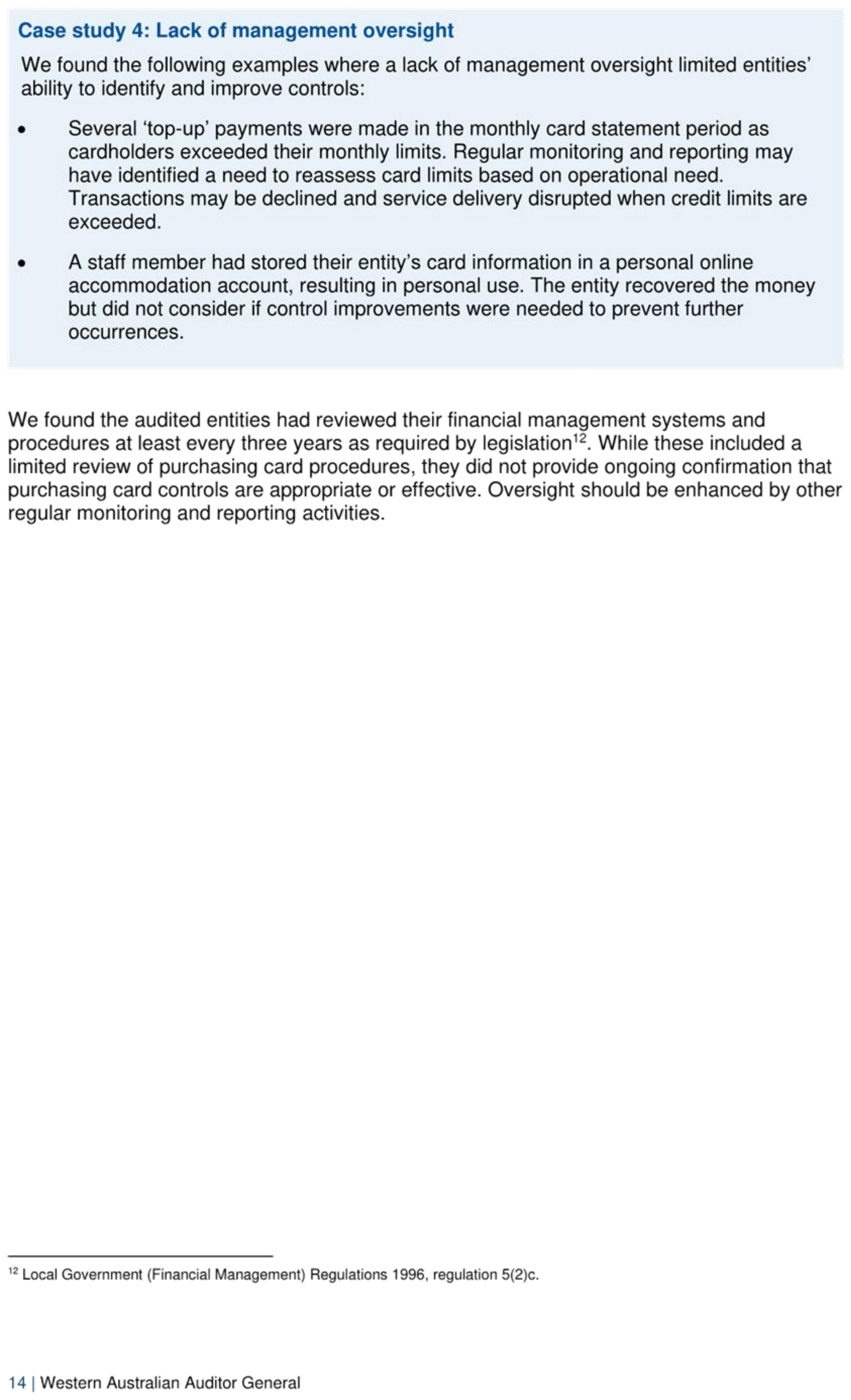
There is an increased likelihood of inadvertent or deliberate misuse and financial loss to entities when cards are not appropriately issued and cancelled.

Lack of appropriate oversight of purchasing card controls

Payment listings provided by the three audited entities to their councils generally met legislated requirements. However, we identified instances where the included descriptions were vague or inaccurate and could have better identified the expenditure to facilitate proper scrutiny.

None of the audited entities had appropriate management oversight of purchasing card control effectiveness. The entities informed us card administrators and line managers did not monitor controls to issue, use and cancel cards or report on shortcomings to management. Regular monitoring would assist entities to identify control gaps and address weaknesses in a timely manner. We noted during the audit that the City of Kalgoorlie-Boulder does have some insight into control effectiveness, but this is limited as it only reviews one month's card use by one randomly selected cardholder as part of its monthly executive meetings.

Case study 4 provides examples that illustrate the need for management oversight over control effectiveness. Our better practice guidance in Appendix 1 provides entities with a range of oversight activities to consider.



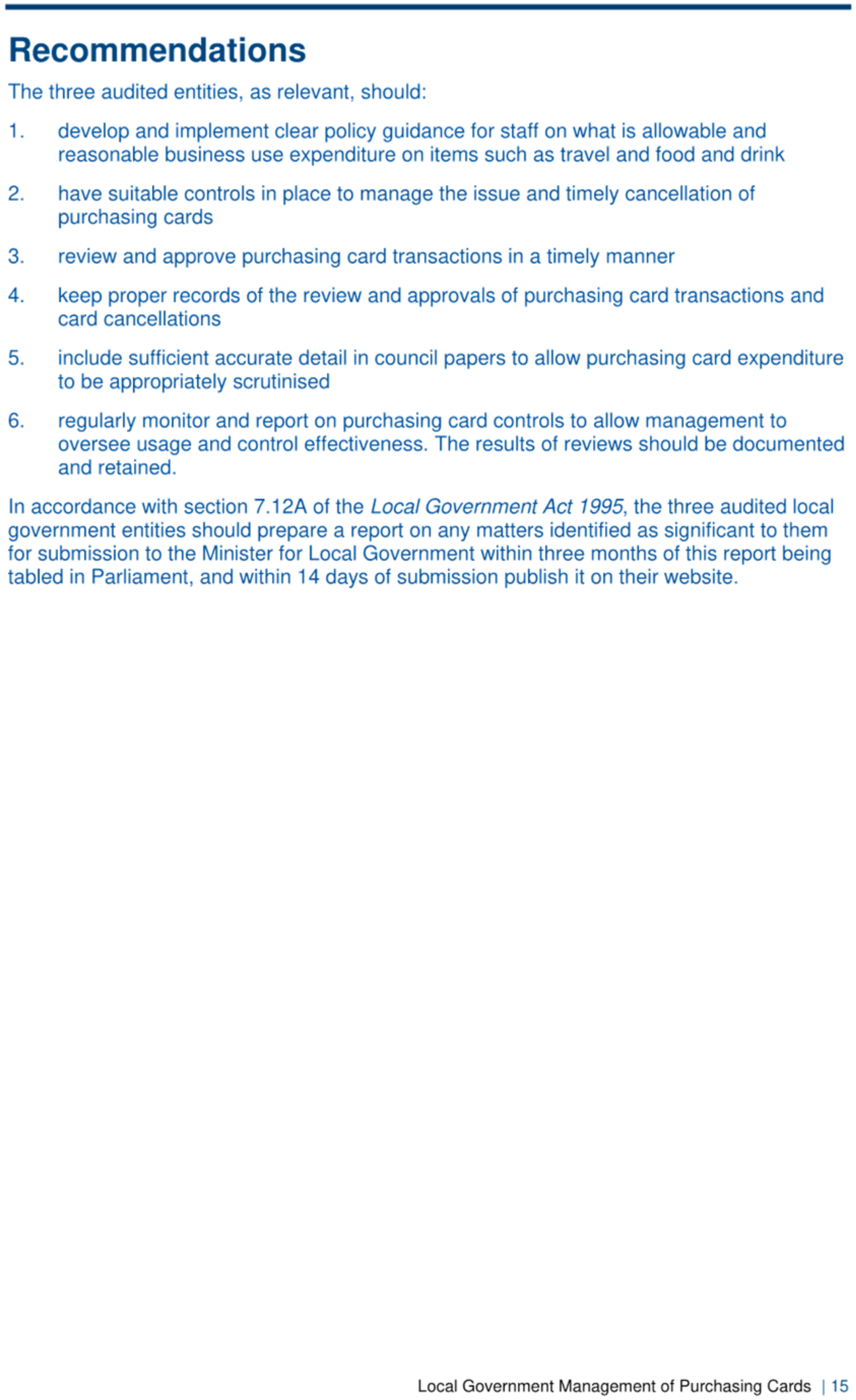
Case study 4: Lack of management oversight

We found the following examples where a lack of management oversight limited entities' ability to identify and improve controls:

- Several 'top-up' payments were made in the monthly card statement period as cardholders exceeded their monthly limits. Regular monitoring and reporting may have identified a need to reassess card limits based on operational need. Transactions may be declined and service delivery disrupted when credit limits are exceeded.
- A staff member had stored their entity's card information in a personal online accommodation account, resulting in personal use. The entity recovered the money but did not consider if control improvements were needed to prevent further occurrences.

We found the audited entities had reviewed their financial management systems and procedures at least every three years as required by legislation[12]. While these included a limited review of purchasing card procedures, they did not provide ongoing confirmation that purchasing card controls are appropriate or effective. Oversight should be enhanced by other regular monitoring and reporting activities.

[12] Local Government (Financial Management) Regulations 1996, regulation 5(2)c.

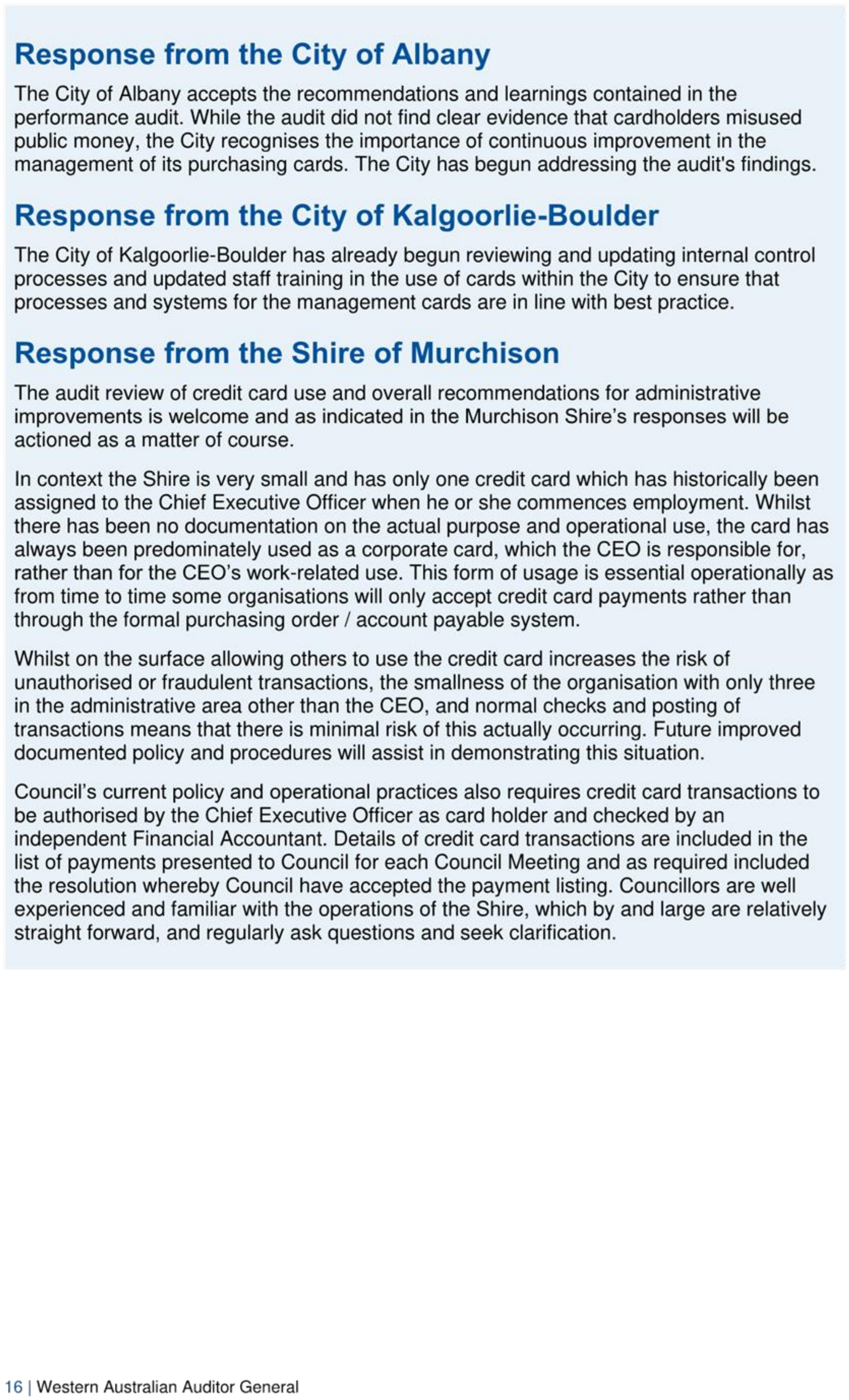


Recommendations

The three audited entities, as relevant, should:

1. develop and implement clear policy guidance for staff on what is allowable and reasonable business use expenditure on items such as travel and food and drink
2. have suitable controls in place to manage the issue and timely cancellation of purchasing cards
3. review and approve purchasing card transactions in a timely manner
4. keep proper records of the review and approvals of purchasing card transactions and card cancellations
5. include sufficient accurate detail in council papers to allow purchasing card expenditure to be appropriately scrutinised
6. regularly monitor and report on purchasing card controls to allow management to oversee usage and control effectiveness. The results of reviews should be documented and retained.

In accordance with section 7.12A of the *Local Government Act 1995*, the three 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 City of Albany

The City of Albany accepts the recommendations and learnings contained in the performance audit. While the audit did not find clear evidence that cardholders misused public money, the City recognises the importance of continuous improvement in the management of its purchasing cards. The City has begun addressing the audit's findings.

Response from the City of Kalgoorlie-Boulder

The City of Kalgoorlie-Boulder has already begun reviewing and updating internal control processes and updated staff training in the use of cards within the City to ensure that processes and systems for the management cards are in line with best practice.

Response from the Shire of Murchison

The audit review of credit card use and overall recommendations for administrative improvements is welcome and as indicated in the Murchison Shire's responses will be actioned as a matter of course.

In context the Shire is very small and has only one credit card which has historically been assigned to the Chief Executive Officer when he or she commences employment. Whilst there has been no documentation on the actual purpose and operational use, the card has always been predominately used as a corporate card, which the CEO is responsible for, rather than for the CEO's work-related use. This form of usage is essential operationally as from time to time some organisations will only accept credit card payments rather than through the formal purchasing order / account payable system.

Whilst on the surface allowing others to use the credit card increases the risk of unauthorised or fraudulent transactions, the smallness of the organisation with only three in the administrative area other than the CEO, and normal checks and posting of transactions means that there is minimal risk of this actually occurring. Future improved documented policy and procedures will assist in demonstrating this situation.

Council's current policy and operational practices also requires credit card transactions to be authorised by the Chief Executive Officer as card holder and checked by an independent Financial Accountant. Details of credit card transactions are included in the list of payments presented to Council for each Council Meeting and as required included the resolution whereby Council have accepted the payment listing. Councillors are well experienced and familiar with the operations of the Shire, which by and large are relatively straight forward, and regularly ask questions and seek clarification.

Audit focus and scope

The focus of this audit was to assess whether three regional local government entities effectively manage the issue, use and cancellation of purchasing cards.

Our criteria were:

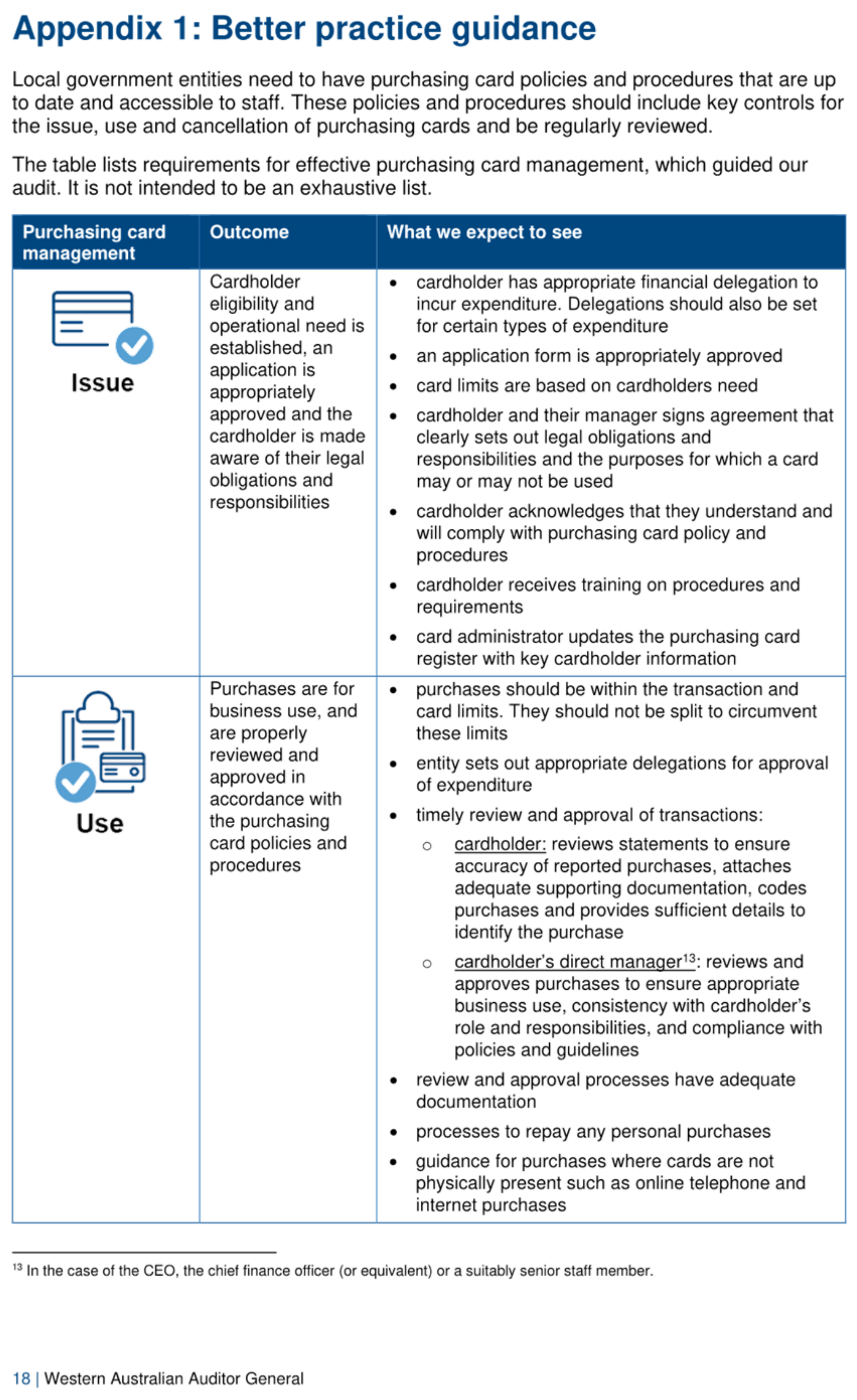
- Are there effective controls over the issue and cancellation of purchasing cards?
- Are there effective controls over the use of purchasing cards?

The City of Albany, City of Kalgoorlie-Boulder and Shire of Murchison were included in the audit.

The audit reviewed the issue, use and cancellation practices of each entity over the period of 1 November 2022 to 31 December 2023.

We visited each entity and assessed their policies and procedures against legislative requirements, DLGSC operational guidelines and our better practice guidance in Appendix 1. At each entity, we also assessed a sample of CEO purchasing card transactions and whether there was adequate independent review of CEO use.

This was an independent 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 of entity programs and activities including compliance with legislative and other requirements. The approximate cost of undertaking the audit and reporting was $300,000.



Appendix 1: Better practice guidance

Local government entities need to have purchasing card policies and procedures that are up to date and accessible to staff. These policies and procedures should include key controls for the issue, use and cancellation of purchasing cards and be regularly reviewed.

The table lists requirements for effective purchasing card management, which guided our audit. It is not intended to be an exhaustive list.

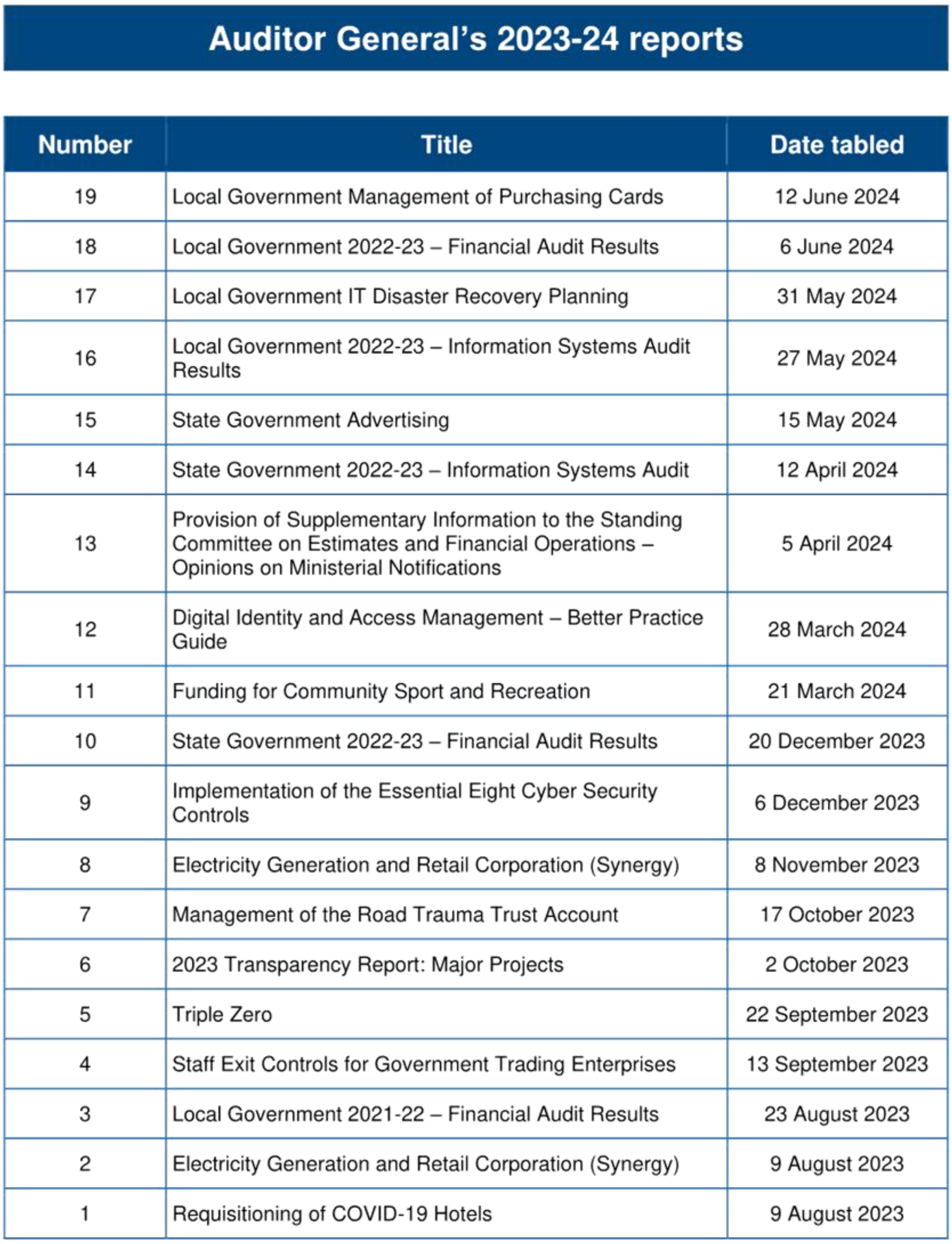
Purchasing card management	Outcome	What we expect to see
Issue	Cardholder eligibility and operational need is established, an application is appropriately approved and the cardholder is made aware of their legal obligations and responsibilities	• cardholder has appropriate financial delegation to incur expenditure. Delegations should also be set for certain types of expenditure • an application form is appropriately approved • card limits are based on cardholders need • cardholder and their manager signs agreement that clearly sets out legal obligations and responsibilities and the purposes for which a card may or may not be used • cardholder acknowledges that they understand and will comply with purchasing card policy and procedures • cardholder receives training on procedures and requirements • card administrator updates the purchasing card register with key cardholder information
Use	Purchases are for business use, and are properly reviewed and approved in accordance with the purchasing card policies and procedures	• purchases should be within the transaction and card limits. They should not be split to circumvent these limits • entity sets out appropriate delegations for approval of expenditure • timely review and approval of transactions: ○ cardholder: reviews statements to ensure accuracy of reported purchases, attaches adequate supporting documentation, codes purchases and provides sufficient details to identify the purchase ○ cardholder's direct manager[13]: reviews and approves purchases to ensure appropriate business use, consistency with cardholder's role and responsibilities, and compliance with policies and guidelines • review and approval processes have adequate documentation • processes to repay any personal purchases • guidance for purchases where cards are not physically present such as online telephone and internet purchases

[13] In the case of the CEO, the chief finance officer (or equivalent) or a suitably senior staff member.

Purchasing card management	Outcome	What we expect to see
		• treatment of reward schemes and loyalty programs as purchasing cards should not be used to gain a personal benefit • procedures for when a cardholder is on leave to ensure card security
Cancellation	Timely cancellation of purchasing cards to prevent unauthorised purchases and unnecessary card fees	• immediate cancellation once a cardholder exits or has a change in employment requirements • cardholder returns card to the administrator • cards should be destroyed, and evidence of destruction recorded • administrator enters cancellation and destruction information in cardholder register
Oversight	Regular monitoring and reporting to provide management with insights into use and the effectiveness of controls and to address shortcomings in a timely manner Evidence of reviews should be retained	Examples of monitoring and reporting include: • Continuously: ○ disclose information about each purchasing card transaction in a payments listing to council and in council minutes ○ record instances of personal use, inappropriate use, and disputed and fraudulent transactions. Take corrective action when required ○ assess the timeliness of reviews and approvals by cardholders and managers, and act when timeframes are not met ○ provide reports to managers on usage within their areas to assess operational need ○ reinforce requirements to cardholders and approvers • Annually: ○ identify inactive or under-used cards that may require cancellation ○ review appropriateness of transaction and card limits ○ audit and update purchasing card registers ○ review relevance and effectiveness of policies and procedures as part of an annual risk assessment • Periodically: ○ sample test transactions for appropriate business use and compliance with policies and procedures ○ analyse usage and supplier patterns to inform procurement practices ○ review purchasing card policy against operational guidelines and better practice principles

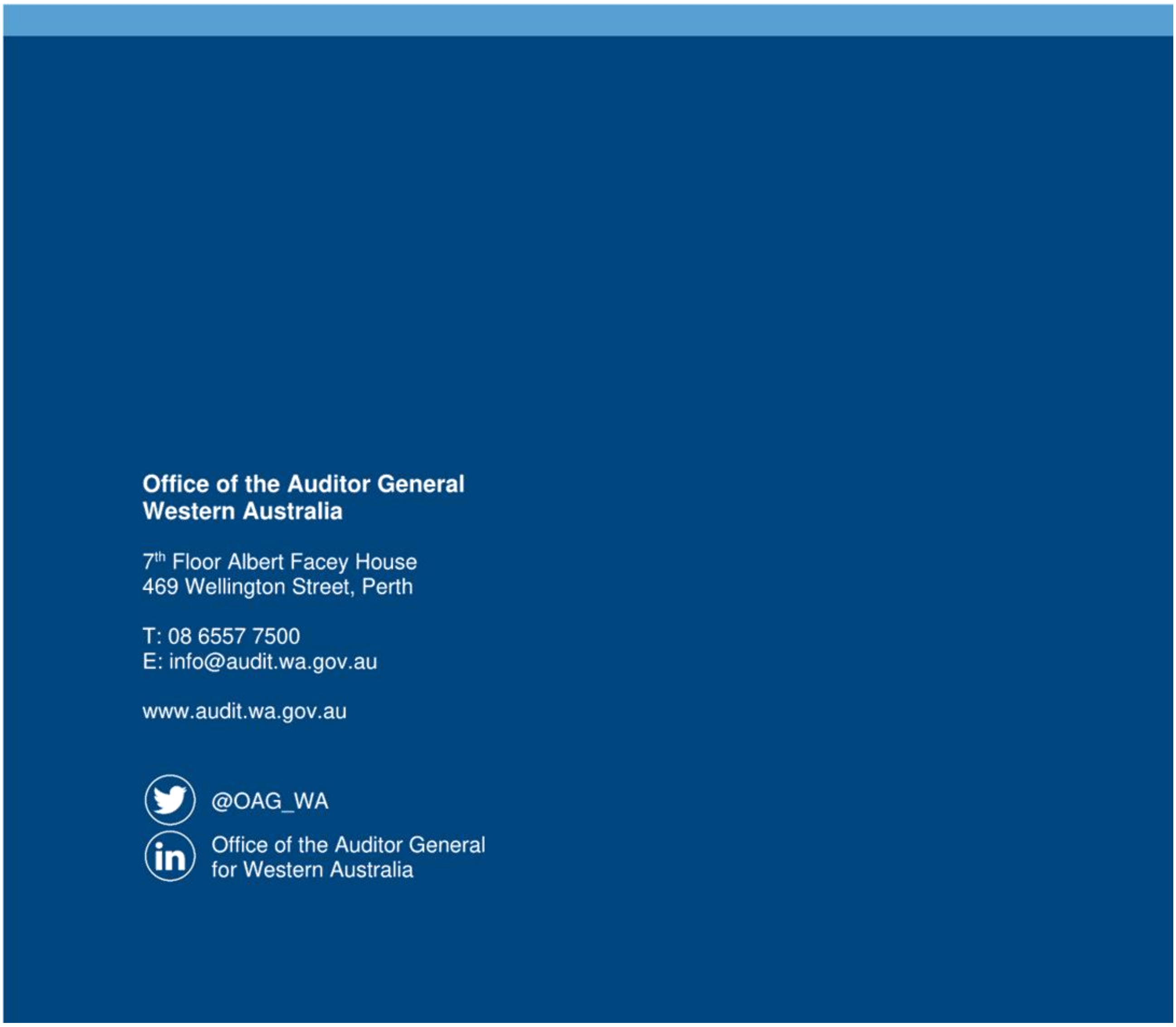
Purchasing card management	Outcome	What we expect to see
		○ review the appropriateness and effectiveness of financial management systems and procedures as required by legislation

Source: OAG



Auditor General's 2023-24 reports

Number	Title	Date tabled
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	State Government 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

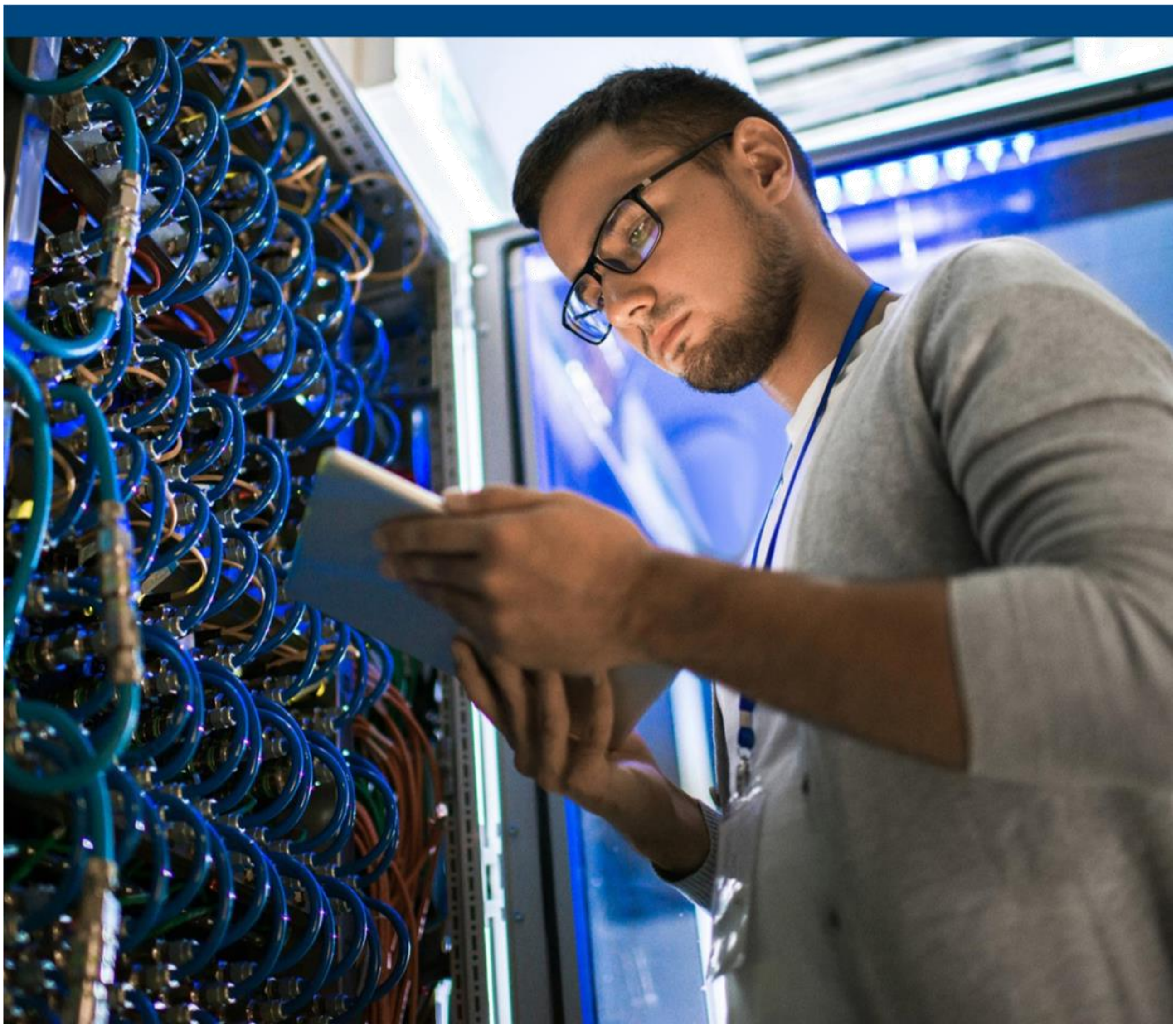
Office of the Auditor General
for Western Australia

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.

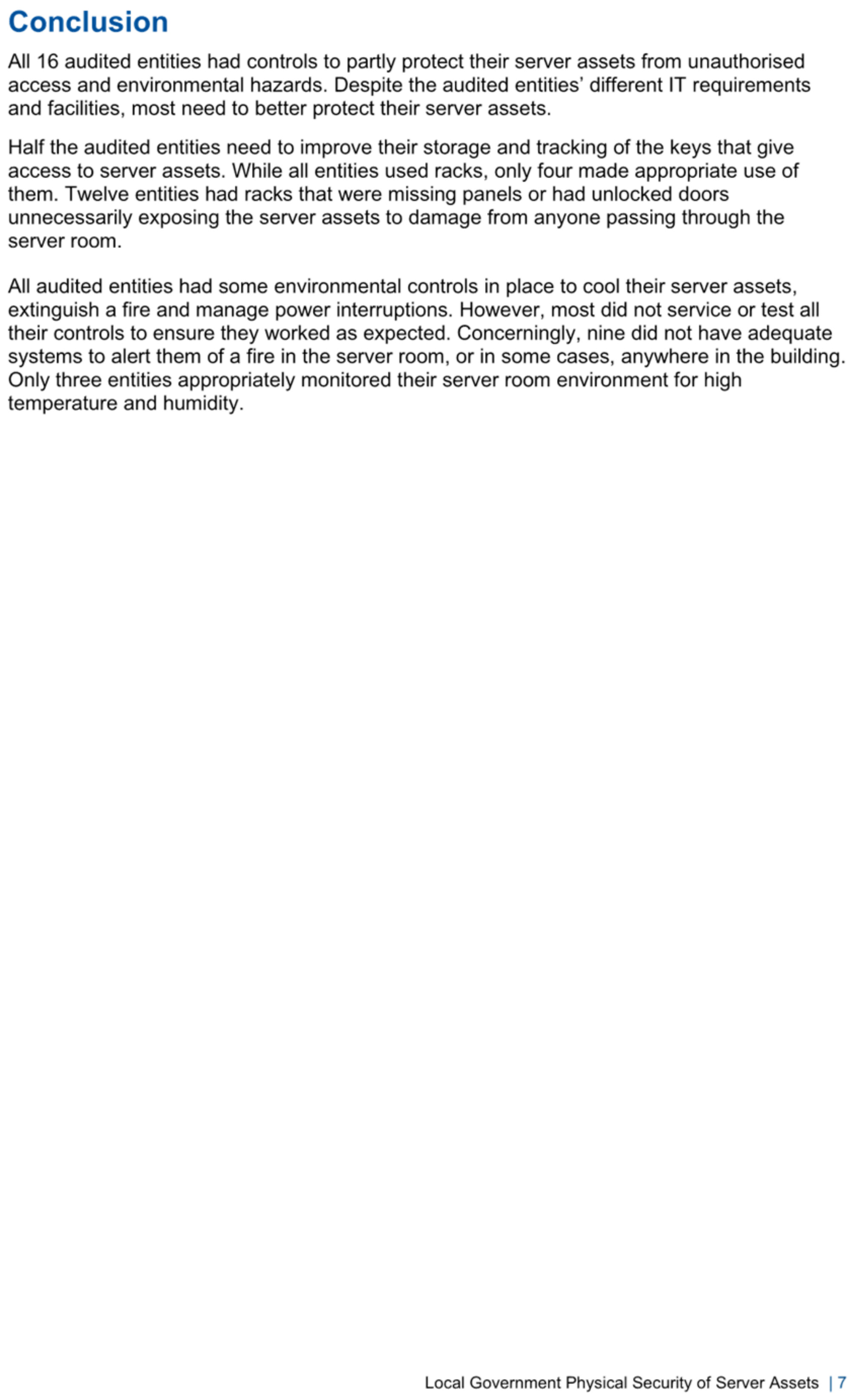
It is good practice to house racks in a dedicated server room. However, when this is not possible, and server assets are housed in shared spaces, they require additional controls such as cages to prevent unauthorised access.

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:

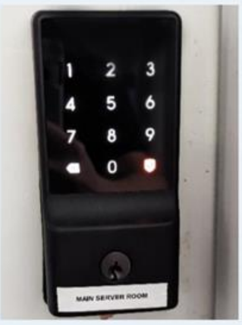
- Physical keys kept in easily accessed areas such as office drawers, in the rack door lock, or on pegs next to the server rack.
- A record of who used physical keys to access server assets was not maintained. Without this kind of record, entities cannot easily track when physical keys are used and returned.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



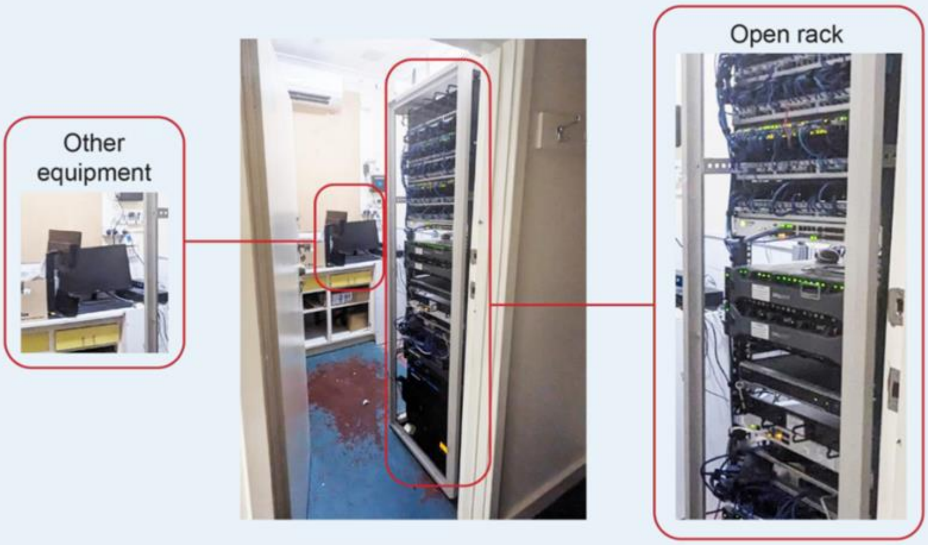
Source: OAG

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.

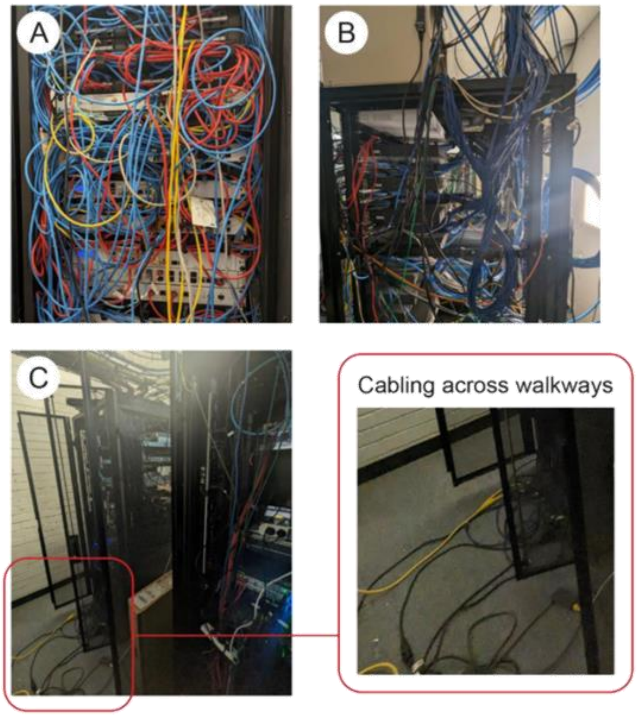
Network and power cabling could be improved

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

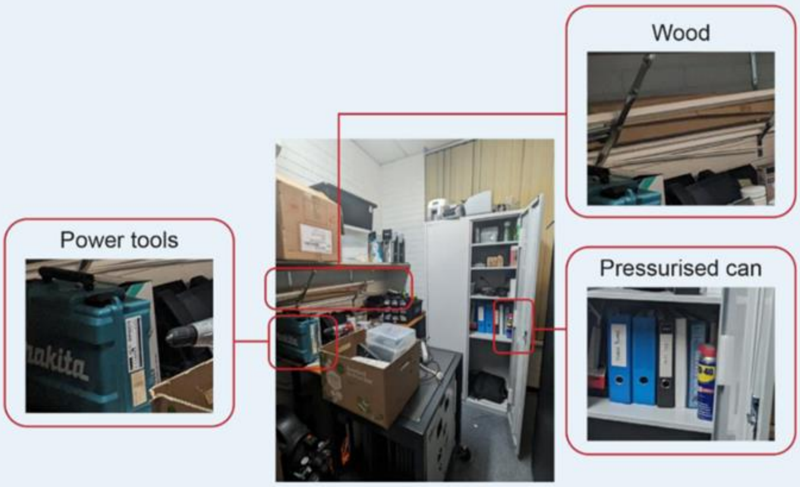
Server rooms are not kept clear of other hazards

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.

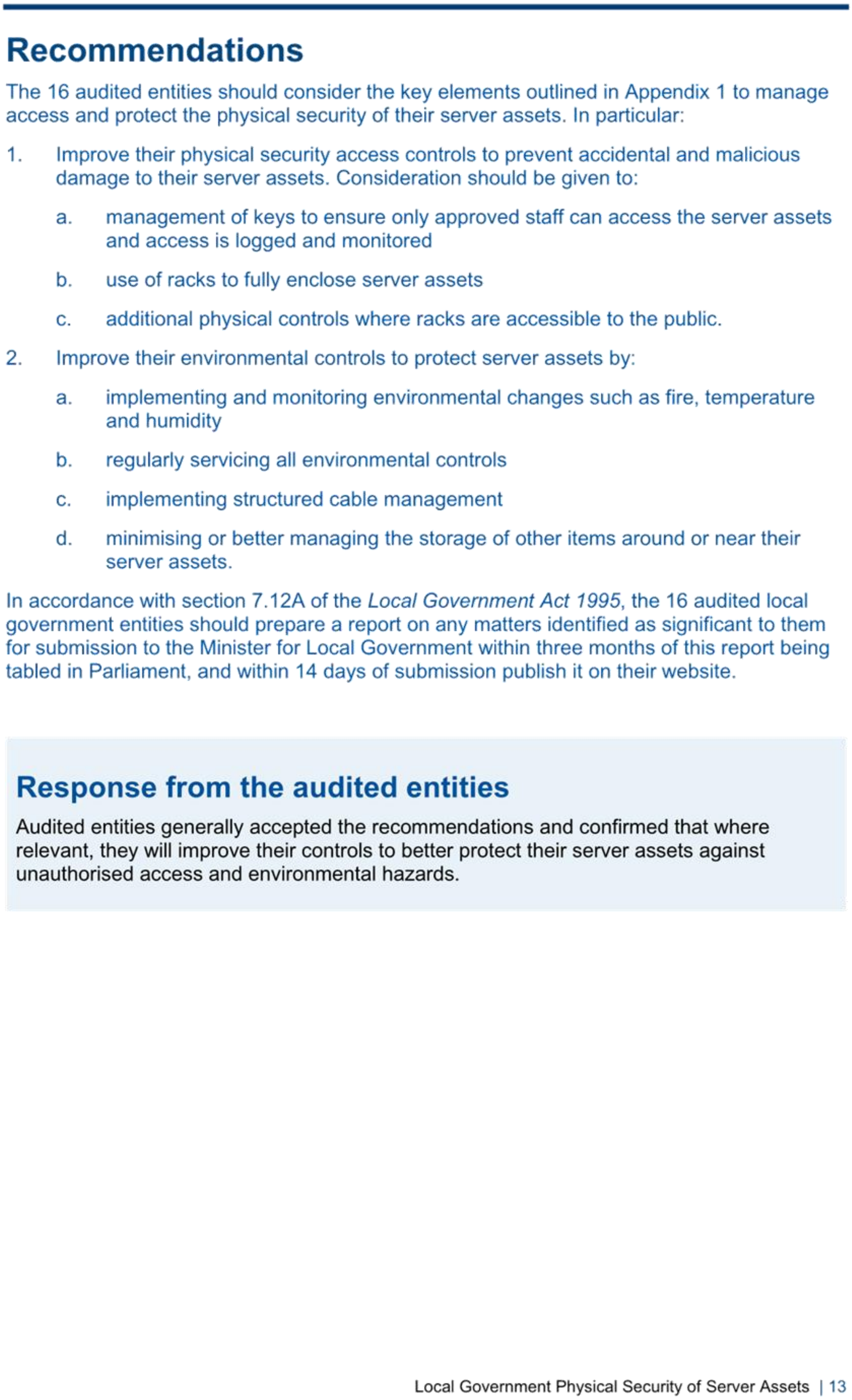
Case study 4: Excess items stored in the room could increase the risk and extent of a fire



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

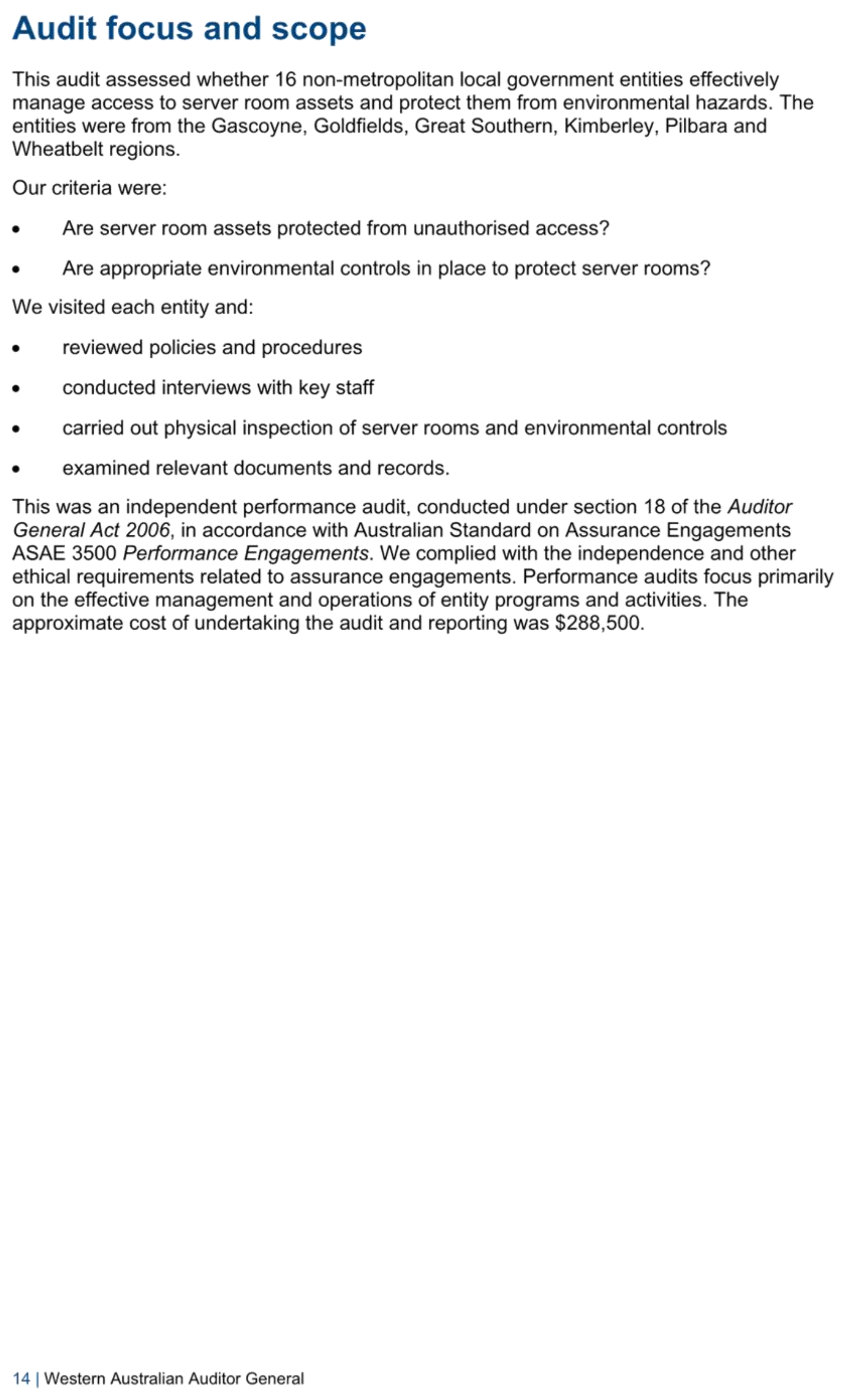
The 16 audited entities should consider the key elements outlined in Appendix 1 to manage access and protect the physical security of their server assets. In particular:

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.

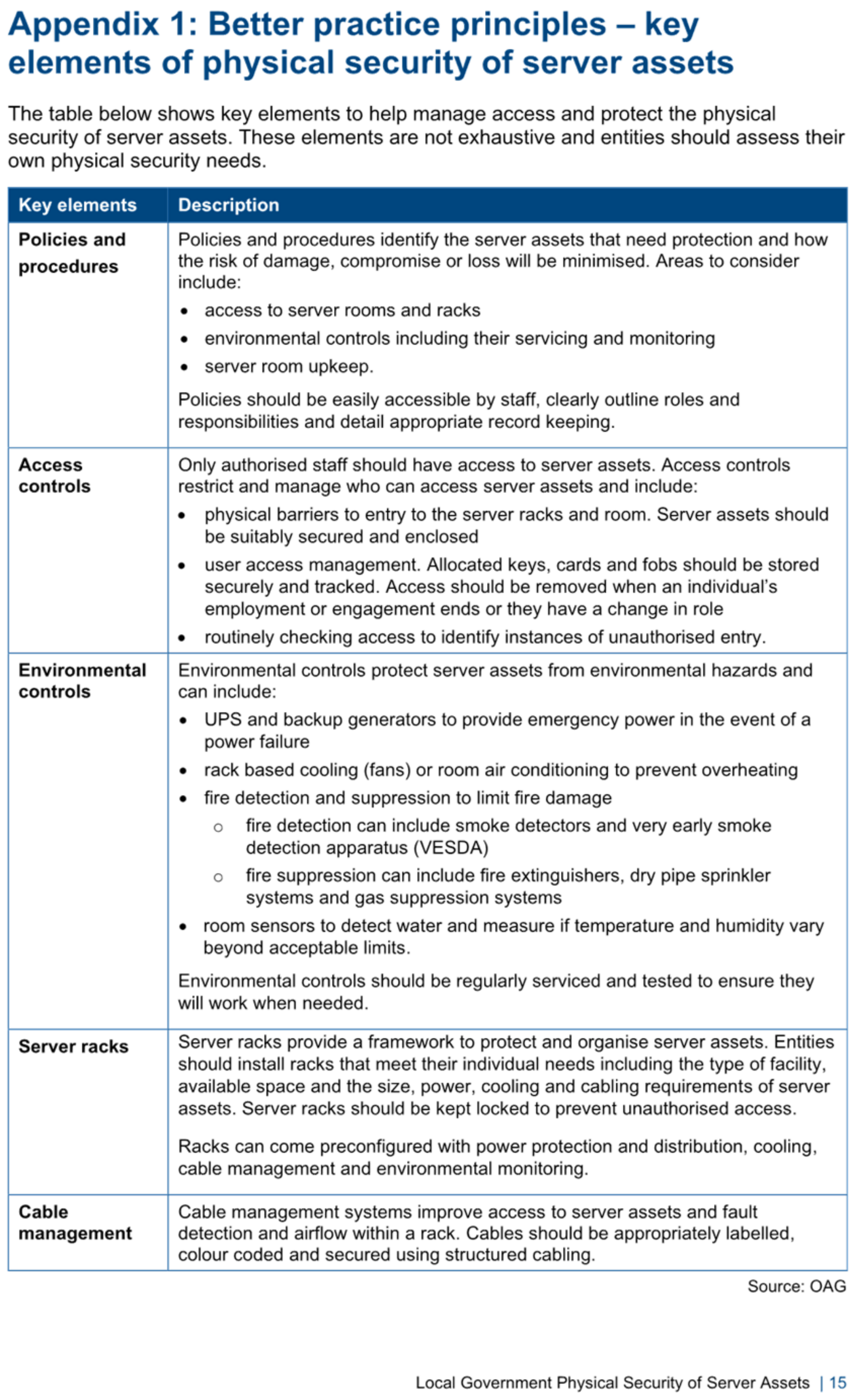
Our criteria were:

- 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.

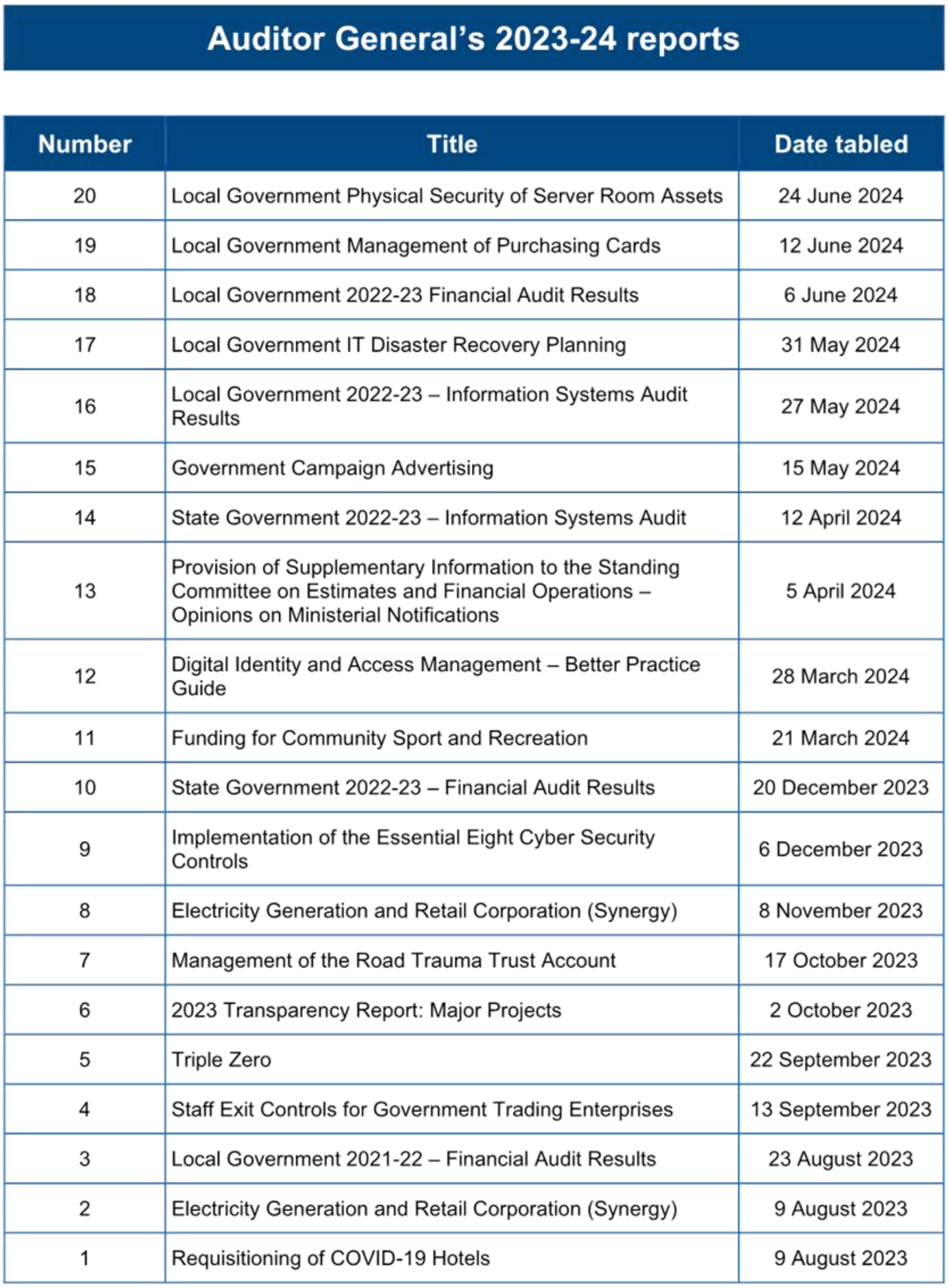


Appendix 1: Better practice principles – key elements of physical security of server assets

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.

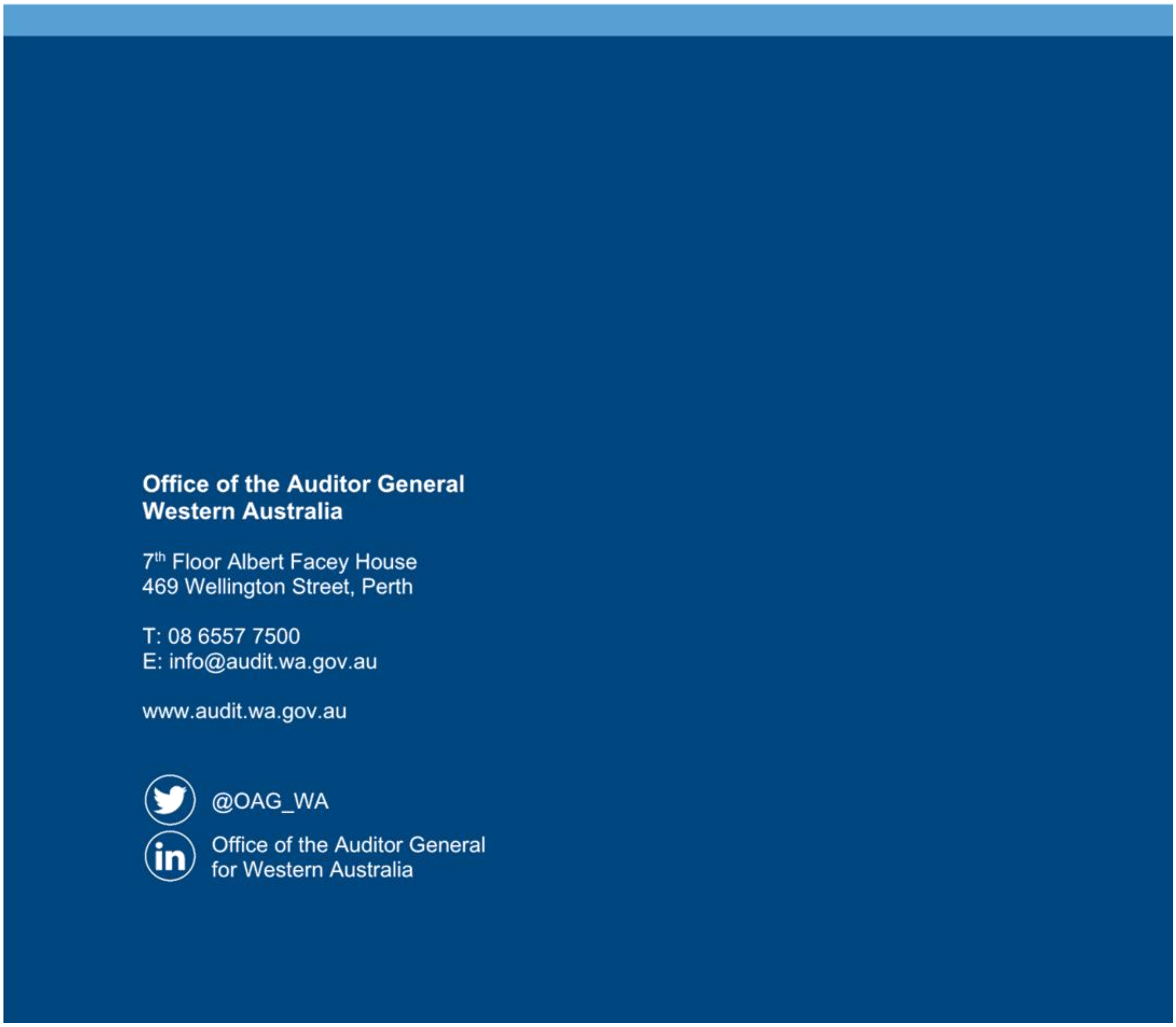
Key elements	Description
Policies and procedures	Policies and procedures identify the server assets that need protection and how the risk of damage, compromise or loss will be minimised. Areas to consider include: • access to server rooms and racks • environmental controls including their servicing and 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

Office of the Auditor General
Serving the Public Interest

Report 25: 2023-24 | 28 June 2024

PERFORMANCE AUDIT

Staff Exit Controls at Large Local Government Entities

Office of the Auditor General
for Western Australia

Audit team:
This audit was conducted by Paxon Group engaged under section 29 of the *Auditor General Act 2006*.

The audit was conducted under the direction of Nayna Raniga and Andrew Harris.

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/iLixe48

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Staff Exit Controls at Large Local Government Entities

Report 25: 2023-24
28 June 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

STAFF EXIT CONTROLS AT LARGE LOCAL GOVERNMENT ENTITIES

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 eight large metropolitan local government entities effectively and efficiently manage the exit of staff to minimise security, asset and financial risks.

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

Caroline Spencer
Auditor General
28 June 2024

Contents

Auditor General's overview

This audit assessed the effectiveness of staff exit controls at eight large metropolitan local government entities. It follows similar audits in both State government entities and government trading enterprises (GTE). The eight entities employ a large number of staff, often across multiple locations, many of whom are casual and temporary employees. In our audit period they also incurred significant staff turnover.

Overall we found that payroll and finance controls were largely effective, but physical security and information technology risks were not always minimised and there were gaps in the documentation of the return of assets. Although this exposes the entities to increased risk, I am pleased that we did not find any instances where information systems had been accessed inappropriately or where assets had been lost or stolen.

All the entities had processes in place for staff exits but their maturity and design varied. Similar to State government entities and GTEs we found that they did not effectively document the assessment of risk and adjust controls to take account of staff leaving high integrity positions.

The risks and challenges identified in my report are not confined to the eight entities we audited. I encourage all public sector entities to look at the findings and recommendations in this report, and draw on the better practice guidance provided in Appendix 1. These should be applied by entities to meet their operational requirements to ensure they have effective staff exit controls in place.

Executive summary

Introduction

Our Office regularly conducts audits to ensure that controls are effective and working as intended. Our recent audits of staff exit controls in State government entities and government trading enterprises (GTE) found access to work premises and information technology (IT) were not consistently cancelled immediately, and exit controls were not assessed for risk and were not adjusted for high integrity positions.

This audit assessed whether eight large metropolitan local government entities (entities) effectively and efficiently manage the exit of staff to minimise security, asset and financial risks. We considered if these entities have appropriate policies and procedures, and whether these are complied with to effectively manage staff exits. This report names local government entities in highlighting good practice and areas to improve. These learnings can be applied more broadly across local government entities and the public sector. Entities have not been named where financial controls are applicable.

Background

The risks relating to staff exits are common to all public sector entities. The local government sector is no exception. It employs a large number of staff, often across multiple locations, many of whom are casual and temporary employees. Entities often see large movements in staff. Our audit covered staff exits during the period 1 January 2023 to 31 December 2023 (Table 1).

City	Headcount	Total staff exits	Casual and temporary staff exits	Permanent staff exits
Armadale	701	213	100	113
Canning	813	270	125	145
Gosnells	671	112	47	65
Joondalup	1,014	207	134	73
Rockingham	725	194	88	106
Stirling	1,490	289	169	120
Swan	1,118	235	67	168
Wanneroo	957	187	43	144
Total	**7,489**	**1,707**	**773**	**934**

Source: OAG using audited entity information

Table 1: Headcount and the number of staff exits at the eight local government entities in 2023

Entities need to ensure when a staff member leaves that premises and information are protected, and all public assets recovered. Ineffective controls increase the risk of security breaches and the loss of information, physical assets and public money.

When staff leave by resignation, retirement, end of contract or through dismissal the entity should:

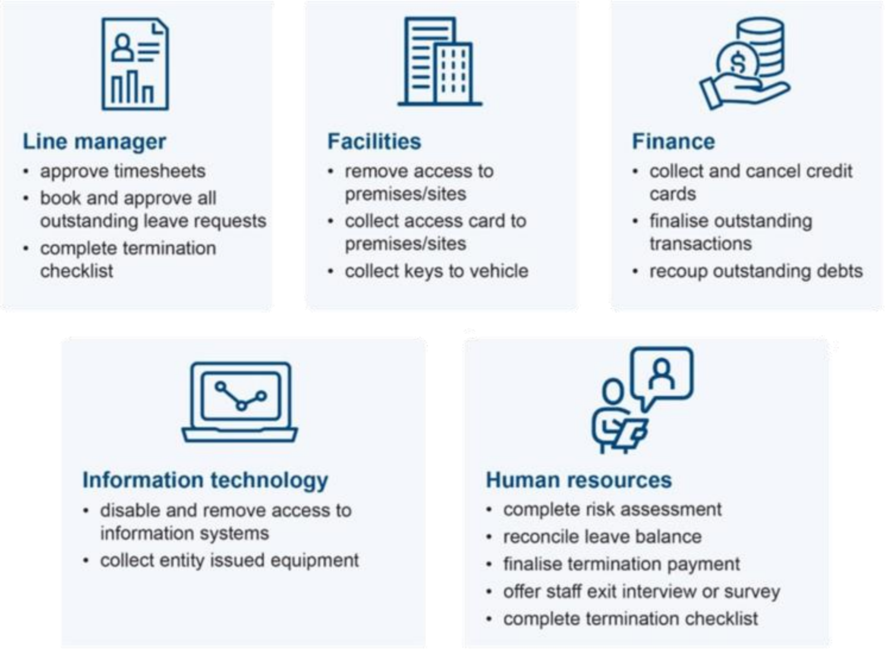
- immediately cancel access to information systems, premises and confidential information

- revoke all physical controls such as identity cards, security access passes (fobs or cards) and keys
- collect all entity owned property
- offer exit interviews
- issue a reminder of the individual's ongoing obligations not to disclose entity information.

Entities should also consider and assess risks presented by staff leaving high integrity positions, or are terminated for misconduct or other adverse reasons. Risk assessments help entities to identify and understand security implications and reduce risks to information, assets and finances. Information to assist entities to manage these risks is included in Appendix 1.

Risk assessments are better managed by adopting a systematic approach that is documented in exit procedures and checklists used by entities. This includes considering post-employment integrity risks and making clear the ongoing requirement for staff to maintain security of information and return all IT assets when the person's employment ends.[1]

To manage staff exits effectively entities require policies and procedures that coordinate activities across multiple business units (these can include human resources, payroll, finance, security, IT and fleet). Entities also need to monitor staff exits to ensure compliance with their policies and procedures, and reduce risk.



Line manager
- approve timesheets
- book and approve all outstanding leave requests
- complete termination checklist

Facilities
- remove access to premises/sites
- collect access card to premises/sites
- collect keys to vehicle

Finance
- collect and cancel credit cards
- finalise outstanding transactions
- recoup outstanding debts

Information technology
- disable and remove access to information systems
- collect entity issued equipment

Human resources
- complete risk assessment
- reconcile leave balance
- finalise termination payment
- offer staff exit interview or survey
- complete termination checklist

Source: OAG using audited entity process maps and information

Note: The business unit names and configurations may vary at different entities.

Figure 1: Five key business units generally involved in the staff exit management process

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

Conclusion

The entities we audited were partly effective in managing staff exits to minimise security, asset and financial risks. Payroll and finance controls in all eight entities were largely effective, but physical security and IT risks were not always minimised and there were gaps in the documentation of the return of assets. Although this exposes the entities to increased risk, we did not find any instances where information systems had been accessed inappropriately or where assets had been lost or stolen.

All the entities had processes in place for staff exits but their maturity and design varied. Entities' monitoring and oversight of the completion and effectiveness of exit controls was limited. Documentation of end-to-end processes varied across the eight entities, and only two entities had processes in place which enabled them to monitor that all exit activities have been completed. Data to check whether IT and security access had been cancelled was inadequate in most entities, mainly because the ageing systems in use at these entities lacked effective reporting functionality.

Similar to State government entities and GTEs, local government entities are not yet mature in assessing risk and adjusting staff exit controls to take account of high integrity positions. Factors such as access to confidential information and/or critical systems are not subject to risk assessment and exit controls are not adjusted accordingly. Although exit interviews or surveys were offered, completion rates were low restricting analysis of results. We did find some entities do not review outcomes of exit interviews and surveys. This reduces opportunities to improve business processes and staff retention, which is a key challenge for many entities.

Findings

Access to buildings and IT was not consistently removed on a timely basis when staff left

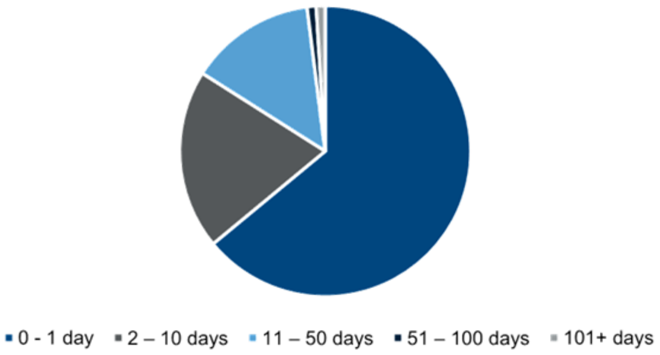
Cancelling access to buildings often took more than a day risking unauthorised access to premises

Physical access cancellation at all eight entities was not always performed on a timely basis, specifically within a day of the employee exit. This exposes the entities to increased risk in terms of unauthorised access to buildings, misappropriation of assets and possible damage to premises.

Almost one third of the staff exits we examined showed access was not cancelled within a day after the employee's last day of employment. We tested 15 exits at each entity.

Across the three entities where data analysis could be performed for the population of exits (Table 2), access was cancelled on a timely basis in 65% of cases, with 35% between two and 101 plus days (Figure 2).

0-1 day	2-10 days	11-50 days	51-100 days	101+ days
65%	20%	13%	1%	1%



Source: OAG based on exit data provided by three local government entities

Figure 2: Days taken to remove physical access

We were able to determine from our sample exits that security cards had been disabled. Processes were also in place for the return of security access cards but we were unable to evidence the return or destruction of these at all eight entities.

In addition to building access cards, some employees also received staff identify cards. At most entities, it was not possible to determine the date of return of identity cards as the cards are destroyed and no documentation is kept. Identity cards allow the holder to exercise powers, such as performing inspections and if they have not been returned and destroyed it increases the risk of them being used inappropriately after someone leaves. This risk is relatively low as there are processes in place to prompt the return of identity cards on staff exit.

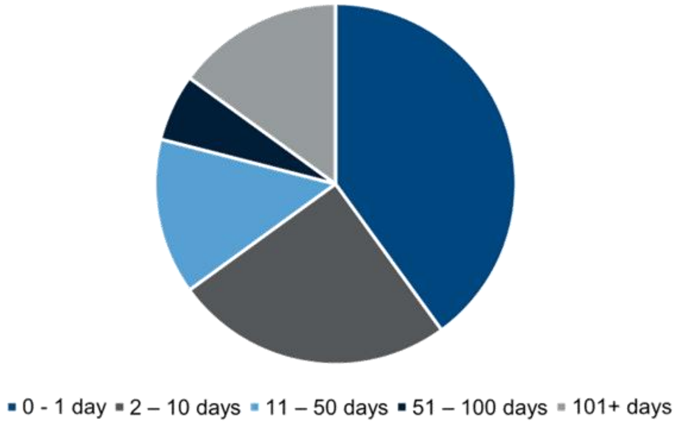
Access to IT was not always cancelled within 24 hours

IT access cancellation was not performed on a timely basis at seven of the eight entities, with 38% of the samples tested not cancelled within 24 hours of staff exit. This increases the risk of inappropriate or unauthorised access being obtained to the entity's information and data. The City of Wanneroo was the only entity where all the exits we tested showed timely cancellation of less than one day.

There were no instances of unauthorised access by an employee after their exit date. We found a very low number of instances of activity on user accounts after exits, but this was approved IT department activity, rather than inappropriate user activity.

Across the six entities where the data allowed us to perform analysis (Table 2), 43% of the total number of exits were timely cancellations but 57% were not, with 4% over 101 days (Figure 3).

0-1 day	2-10 days	11-50 days	51-100 days	101+ days
43%	34%	16%	3%	4%



Source: OAG based on exit data provided by six local government entities

Figure 3: Days taken to remove IT access

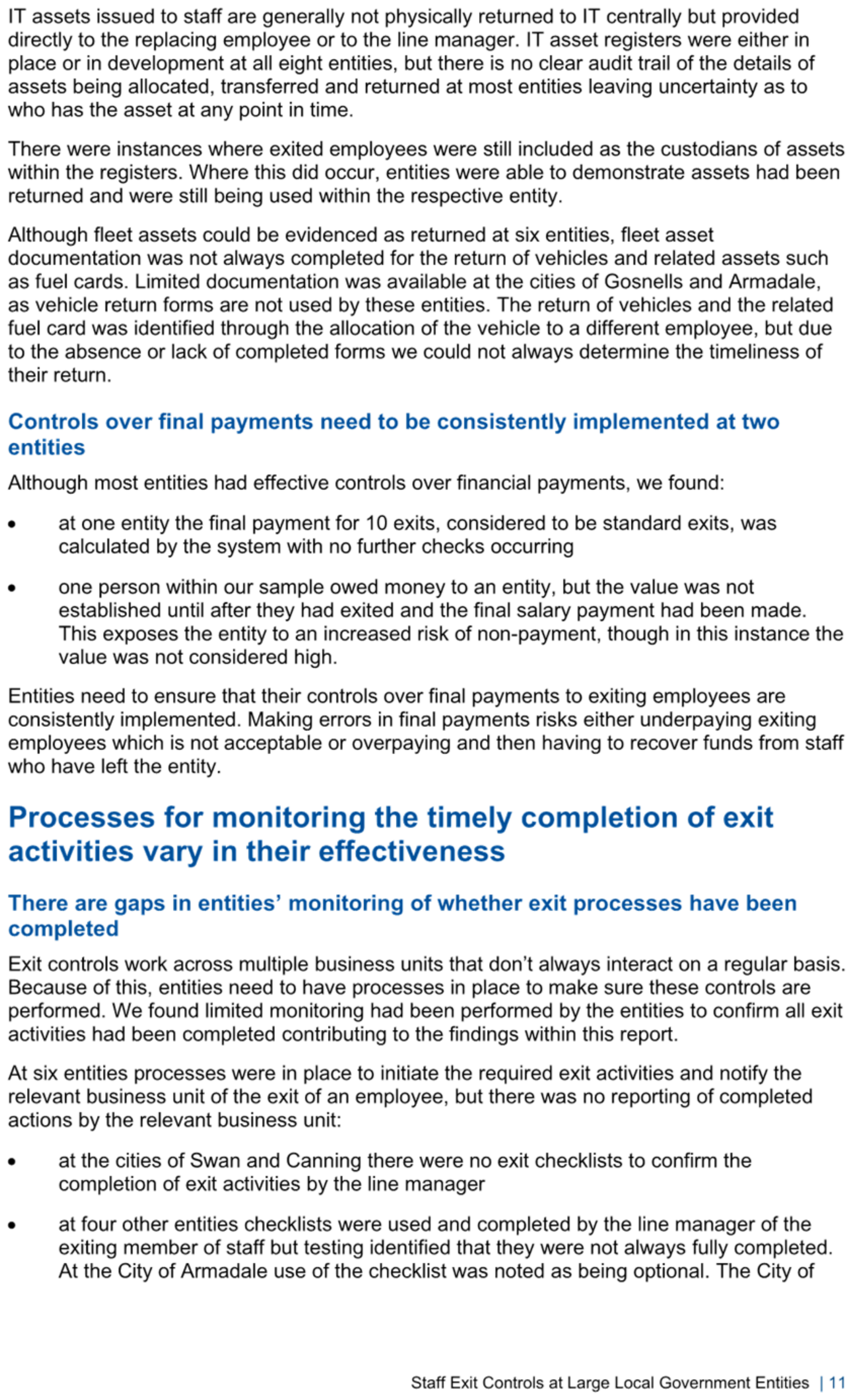
Of the eight entities only the City of Rockingham had defined target timeframes for the cancellation of access to IT and security access cards. It also performed significantly better than the other entities where we were able to analyse the data across the entire population of staff exits.

The return of assets was not always actioned or documented effectively

The return of assets was not always effectively documented

While we did not find any instances where assets had been lost or stolen, it was not possible to confirm that assets allocated to exiting staff were returned at the point of exit.

Although all eight entities have processes to administer the return of assets we found that forms were not always in place or completed to identify which assets had been allocated to which staff, and when they were returned.



IT assets issued to staff are generally not physically returned to IT centrally but provided directly to the replacing employee or to the line manager. IT asset registers were either in place or in development at all eight entities, but there is no clear audit trail of the details of assets being allocated, transferred and returned at most entities leaving uncertainty as to who has the asset at any point in time.

There were instances where exited employees were still included as the custodians of assets within the registers. Where this did occur, entities were able to demonstrate assets had been returned and were still being used within the respective entity.

Although fleet assets could be evidenced as returned at six entities, fleet asset documentation was not always completed for the return of vehicles and related assets such as fuel cards. Limited documentation was available at the cities of Gosnells and Armadale, as vehicle return forms are not used by these entities. The return of vehicles and the related fuel card was identified through the allocation of the vehicle to a different employee, but due to the absence or lack of completed forms we could not always determine the timeliness of their return.

Controls over final payments need to be consistently implemented at two entities

Although most entities had effective controls over financial payments, we found:

- at one entity the final payment for 10 exits, considered to be standard exits, was calculated by the system with no further checks occurring
- one person within our sample owed money to an entity, but the value was not established until after they had exited and the final salary payment had been made. This exposes the entity to an increased risk of non-payment, though in this instance the value was not considered high.

Entities need to ensure that their controls over final payments to exiting employees are consistently implemented. Making errors in final payments risks either underpaying exiting employees which is not acceptable or overpaying and then having to recover funds from staff who have left the entity.

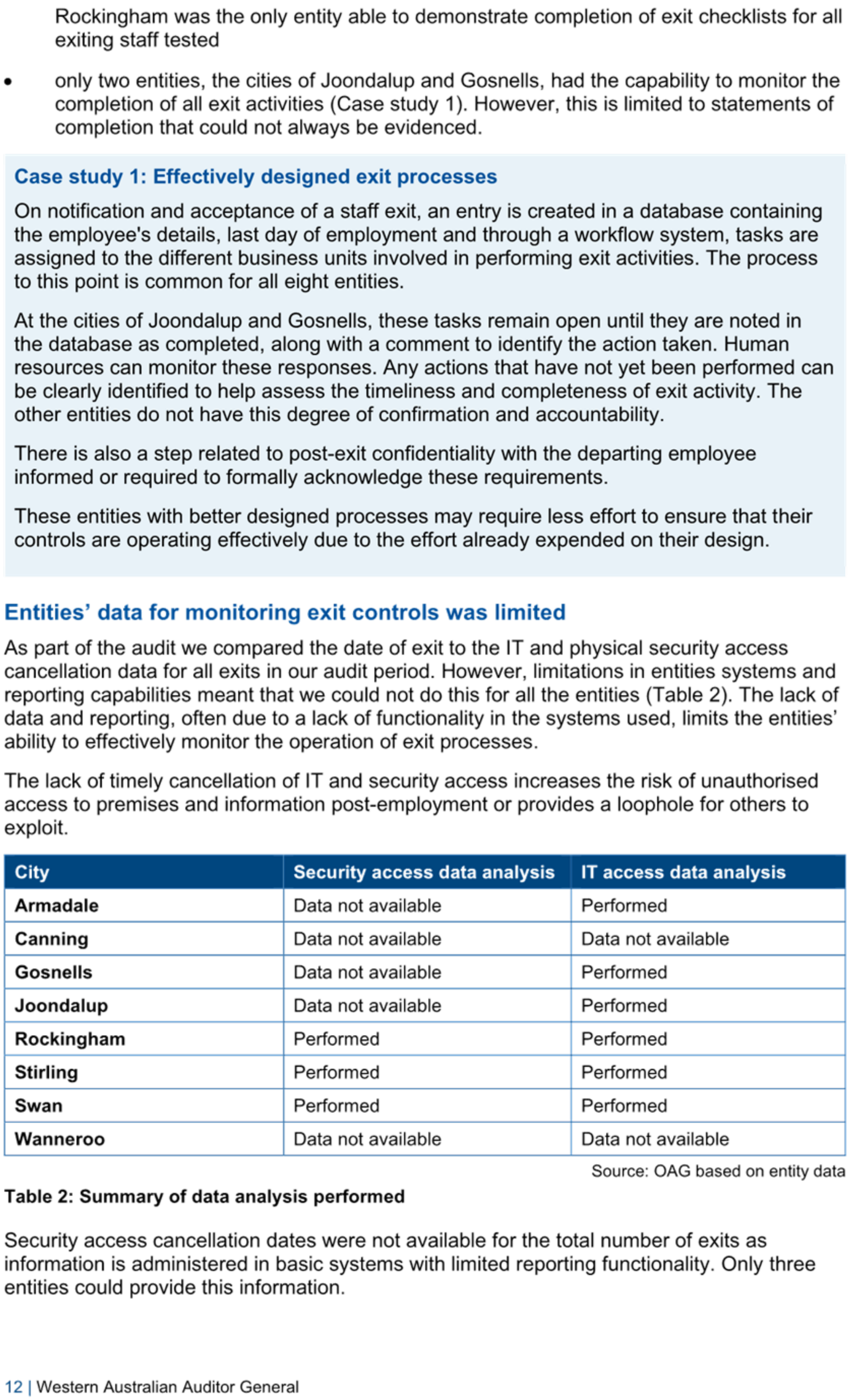
Processes for monitoring the timely completion of exit activities vary in their effectiveness

There are gaps in entities' monitoring of whether exit processes have been completed

Exit controls work across multiple business units that don't always interact on a regular basis. Because of this, entities need to have processes in place to make sure these controls are performed. We found limited monitoring had been performed by the entities to confirm all exit activities had been completed contributing to the findings within this report.

At six entities processes were in place to initiate the required exit activities and notify the relevant business unit of the exit of an employee, but there was no reporting of completed actions by the relevant business unit:

- at the cities of Swan and Canning there were no exit checklists to confirm the completion of exit activities by the line manager
- at four other entities checklists were used and completed by the line manager of the exiting member of staff but testing identified that they were not always fully completed. At the City of Armadale use of the checklist was noted as being optional. The City of



Rockingham was the only entity able to demonstrate completion of exit checklists for all exiting staff tested

- only two entities, the cities of Joondalup and Gosnells, had the capability to monitor the completion of all exit activities (Case study 1). However, this is limited to statements of completion that could not always be evidenced.

Case study 1: Effectively designed exit processes

On notification and acceptance of a staff exit, an entry is created in a database containing the employee's details, last day of employment and through a workflow system, tasks are assigned to the different business units involved in performing exit activities. The process to this point is common for all eight entities.

At the cities of Joondalup and Gosnells, these tasks remain open until they are noted in the database as completed, along with a comment to identify the action taken. Human resources can monitor these responses. Any actions that have not yet been performed can be clearly identified to help assess the timeliness and completeness of exit activity. The other entities do not have this degree of confirmation and accountability.

There is also a step related to post-exit confidentiality with the departing employee informed or required to formally acknowledge these requirements.

These entities with better designed processes may require less effort to ensure that their controls are operating effectively due to the effort already expended on their design.

Entities' data for monitoring exit controls was limited

As part of the audit we compared the date of exit to the IT and physical security access cancellation data for all exits in our audit period. However, limitations in entities systems and reporting capabilities meant that we could not do this for all the entities (Table 2). The lack of data and reporting, often due to a lack of functionality in the systems used, limits the entities' ability to effectively monitor the operation of exit processes.

The lack of timely cancellation of IT and security access increases the risk of unauthorised access to premises and information post-employment or provides a loophole for others to exploit.

City	Security access data analysis	IT access data analysis
Armadale	Data not available	Performed
Canning	Data not available	Data not available
Gosnells	Data not available	Performed
Joondalup	Data not available	Performed
Rockingham	Performed	Performed
Stirling	Performed	Performed
Swan	Performed	Performed
Wanneroo	Data not available	Data not available

Source: OAG based on entity data

Table 2: Summary of data analysis performed

Security access cancellation dates were not available for the total number of exits as information is administered in basic systems with limited reporting functionality. Only three entities could provide this information.

Information relating to security cancellation for individuals was available, however at the City of Canning it was not possible to obtain complete information on individual exit security cancellation dates as they were manually recorded on spreadsheets or information was missing.

At two entities IT access cancellation dates were only available by individual and not for all exits due to system reporting limitations. Improvements in the availability of this data would enable entities' to implement more effective oversight of these areas and perform comparison of the cancellation dates to assess their completeness and timeliness.

Exit controls are not responsive to the risks with exits from high integrity positions and are not effectively documented

Exit controls are not adjusted to reflect high integrity positions and are not effectively documented

None of the entities had a documented process for assessing risk when someone is leaving a high integrity position or could demonstrate additional measures that might be required to manage their exit. For example, controls may need to be adjusted to manage risks or security concerns of staff who are in high integrity positions where they have access to things like confidential information or payroll systems or bank accounts. Measures were in place for higher risk exits where there were performance or disciplinary issues.

Risks are most effectively identified and managed with a systematic approach to assessing them. Risk assessments assist entities to identify security implications and tailor approaches to minimise risks to information, assets and finances. An understanding of the risks and having documented procedures to mitigate them allows adjustments of controls to be made in the staff exit process to match the circumstances. High integrity positions are not always senior positions and risk assessments need to take account of access to information, systems and resources.

At one entity an employee who left was not removed from the bank authorised signatory listing until 105 days after exiting, which increases the risk of unauthorised transactions or access occurring. This may have been mitigated if the increased risk had been considered. In this instance there were mitigating controls with dual signatories required for all administrative changes to bank accounts and the employee did not have access to the banks online system to make transactions. However, this type of delay greatly increases the risk to the entity if the exiting staff member had greater banking access.

Exiting staff were not consistently reminded of their post-employment confidentiality obligations

There was no confidentiality obligation acknowledgement for employees post-exit at six entities. Processes on entry and during employment through the Code of Conduct were in place, but there was no reminder or agreement signed on exit except for the cities of Joondalup and Gosnells.

Entities should ensure that all exiting staff especially those with access to sensitive or classified information are advised and acknowledge their obligation not to disclose entity information even after they leave. This helps safeguard entity resources and limit potential for the integrity, availability and confidentiality of sensitive information to be compromised.

There were gaps in the documentation of exit processes at all the entities

Exit controls are distributed across multiple business units who need to work together to be effective. However, none of the entities had end-to-end documented processes to facilitate the consistency, completeness and timeliness of the operation of exit controls and processes.

High level process documents or team specific documents were in place across the entities, but none of these were comprehensive. The key gaps include:

- exit checklists and completion of process confirmation were not in place at the cities of Swan and Canning
- no specific guidance on the timeliness for performance of activities such as disablement of IT and security access at seven of the eight entities
- lack of information or records for the return or transfer of IT and other assets to evidence what is being transferred, when and to whom, at seven of the eight entities
- no confirmation to exiting employees of resignation acceptance, departure timing and terms at the cities of Swan and Gosnells.

Policy and procedure documents help guide and direct entity staff. They provide a structure for consistency and ensure compliance with regulations and standards. Having incomplete policy and procedure documents makes it hard for entities to align practice with their strategic values and comply with regulations and standards.

Exit surveys and interviews are not frequently completed and there is limited analysis of feedback

Processes for exit interviews and surveys were in place at all entities and were generally offered to all exiting employees, with feedback mechanisms including online surveys and internal forms sent out by email. Only 14 of the 120 exits tested completed the survey and provided feedback, which is a low response rate, although we acknowledge that this is in part because it is a voluntary process. The forms viewed varied in length from 14 to 79 questions, but there was no correlation between length and response.

At seven entities, there were limited or no documented processes to show systematic analysis of results from exit interviews and surveys completed by staff and reported to management to identify improvements. Information from exit interviews and surveys can help entities to assess strengths and vulnerabilities, and focus workforce management strategies to drive talent attraction and retention.

Recommendations

These recommendations are based on the eight entities we audited but are relevant for all local government entities and should be read in conjunction with the staff exit better practice guide at Appendix 1.

1. All entities should:

   a. review and where required document end-to-end policies and procedures for employee terminations

   b. regularly review staff exit information allowing effective oversight and monitoring of end-to-end processes and ensure compliance with policies and procedures.

   Implementation timeframe: December 2024

   Entity response: Supported by local government entities.

2. All entities should evaluate risk posed by different positions and termination types, develop and document procedures to manage the risks effectively and efficiently.

   Implementation timeframe: Ongoing

   Entity response: Supported by local government entities.

3. To minimise the risk of property and information loss all entities should:

   a. ensure access to IT systems, buildings and banking delegations are removed or disabled within 24 hours of the exit date

   b. ensure all assets are returned on or prior to the day of exit

   c. put in place and complete a documented process for the allocation, return and transfer of identifiable assets between custodians to maintain a clear audit trail in asset registers

   d. amounts payable to entities by exiting employees should be settled during final payment or repayment plans should be put in place prior to employees exiting

   e. final payment calculations should be performed and reviewed in a timely manner, with evidence retained.

   Implementation timeframe: Ongoing

   Entity response: Supported by local government entities.

4. All entities should:

   a. offer interviews to and/or survey all exiting staff

   b. assess exit survey feedback processes in an attempt to increase feedback received and perform analysis of feedback received to identify improvement opportunities

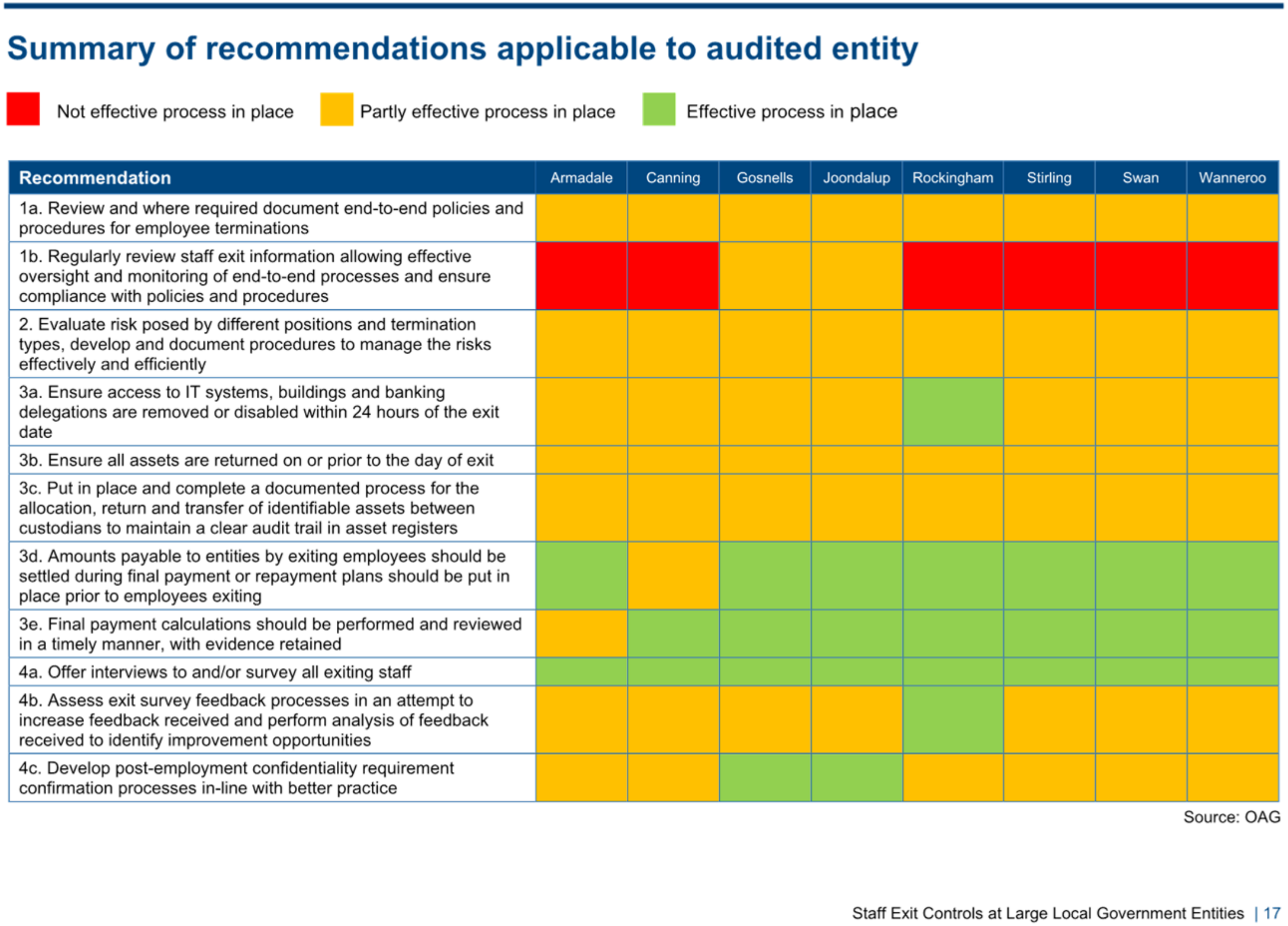
   c. develop post-employment confidentiality requirement confirmation processes in-line with better practice.

   Implementation timeframe: December 2024

   Entity response: Supported by local government entities.

Appendix 2 outlines individual local government entity responses to the recommendations above.

In accordance with section 7.12A of the *Local Government Act 1995*, the eight 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.



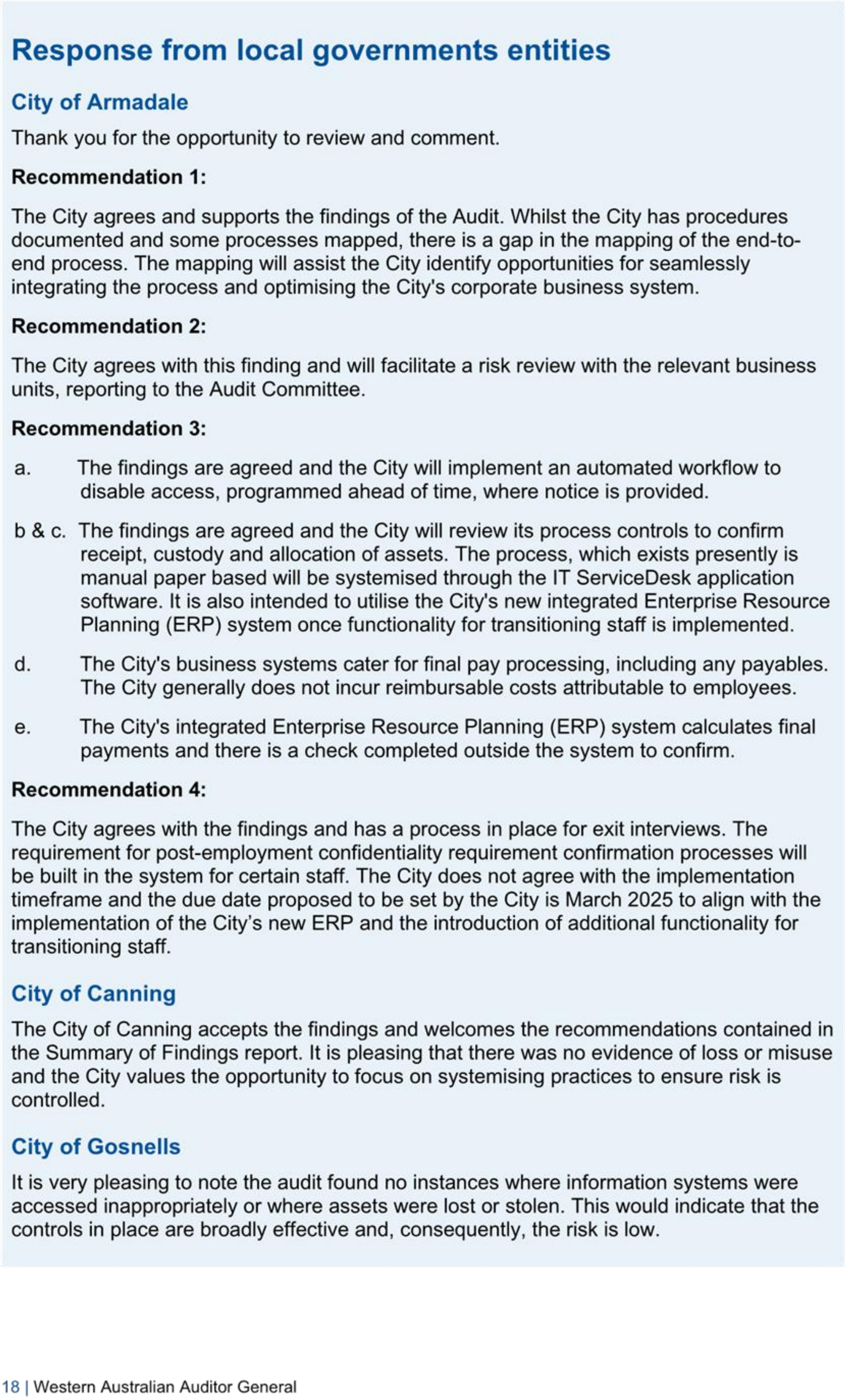
Summary of recommendations applicable to audited entity

🟥 Not effective process in place 🟨 Partly effective process in place 🟩 Effective process in place

Recommendation	Armadale	Canning	Gosnells	Joondalup	Rockingham	Stirling	Swan	Wanneroo
1a. Review and where required document end-to-end policies and procedures for employee terminations	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
1b. Regularly review staff exit information allowing effective oversight and monitoring of end-to-end processes and ensure compliance with policies and procedures	🟥	🟥	🟨	🟨	🟥	🟥	🟥	🟥
2. Evaluate risk posed by different positions and termination types, develop and document procedures to manage the risks effectively and efficiently	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
3a. Ensure access to IT systems, buildings and banking delegations are removed or disabled within 24 hours of the exit date	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟨
3b. Ensure all assets are returned on or prior to the day of exit	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
3c. Put in place and complete a documented process for the allocation, return and transfer of identifiable assets between custodians to maintain a clear audit trail in asset registers	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
3d. Amounts payable to entities by exiting employees should be settled during final payment or repayment plans should be put in place prior to employees exiting	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩
3e. Final payment calculations should be performed and reviewed in a timely manner, with evidence retained	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩
4a. Offer interviews to and/or survey all exiting staff	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
4b. Assess exit survey feedback processes in an attempt to increase feedback received and perform analysis of feedback received to identify improvement opportunities	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟨
4c. Develop post-employment confidentiality requirement confirmation processes in-line with better practice	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨

Source: OAG

Staff Exit Controls at Large Local Government Entities | 17



Response from local governments entities

City of Armadale

Thank you for the opportunity to review and comment.

Recommendation 1:

The City agrees and supports the findings of the Audit. Whilst the City has procedures documented and some processes mapped, there is a gap in the mapping of the end-to-end process. The mapping will assist the City identify opportunities for seamlessly integrating the process and optimising the City's corporate business system.

Recommendation 2:

The City agrees with this finding and will facilitate a risk review with the relevant business units, reporting to the Audit Committee.

Recommendation 3:

a. The findings are agreed and the City will implement an automated workflow to disable access, programmed ahead of time, where notice is provided.

b & c. The findings are agreed and the City will review its process controls to confirm receipt, custody and allocation of assets. The process, which exists presently is manual paper based will be systemised through the IT ServiceDesk application software. It is also intended to utilise the City's new integrated Enterprise Resource Planning (ERP) system once functionality for transitioning staff is implemented.

d. The City's business systems cater for final pay processing, including any payables. The City generally does not incur reimbursable costs attributable to employees.

e. The City's integrated Enterprise Resource Planning (ERP) system calculates final payments and there is a check completed outside the system to confirm.

Recommendation 4:

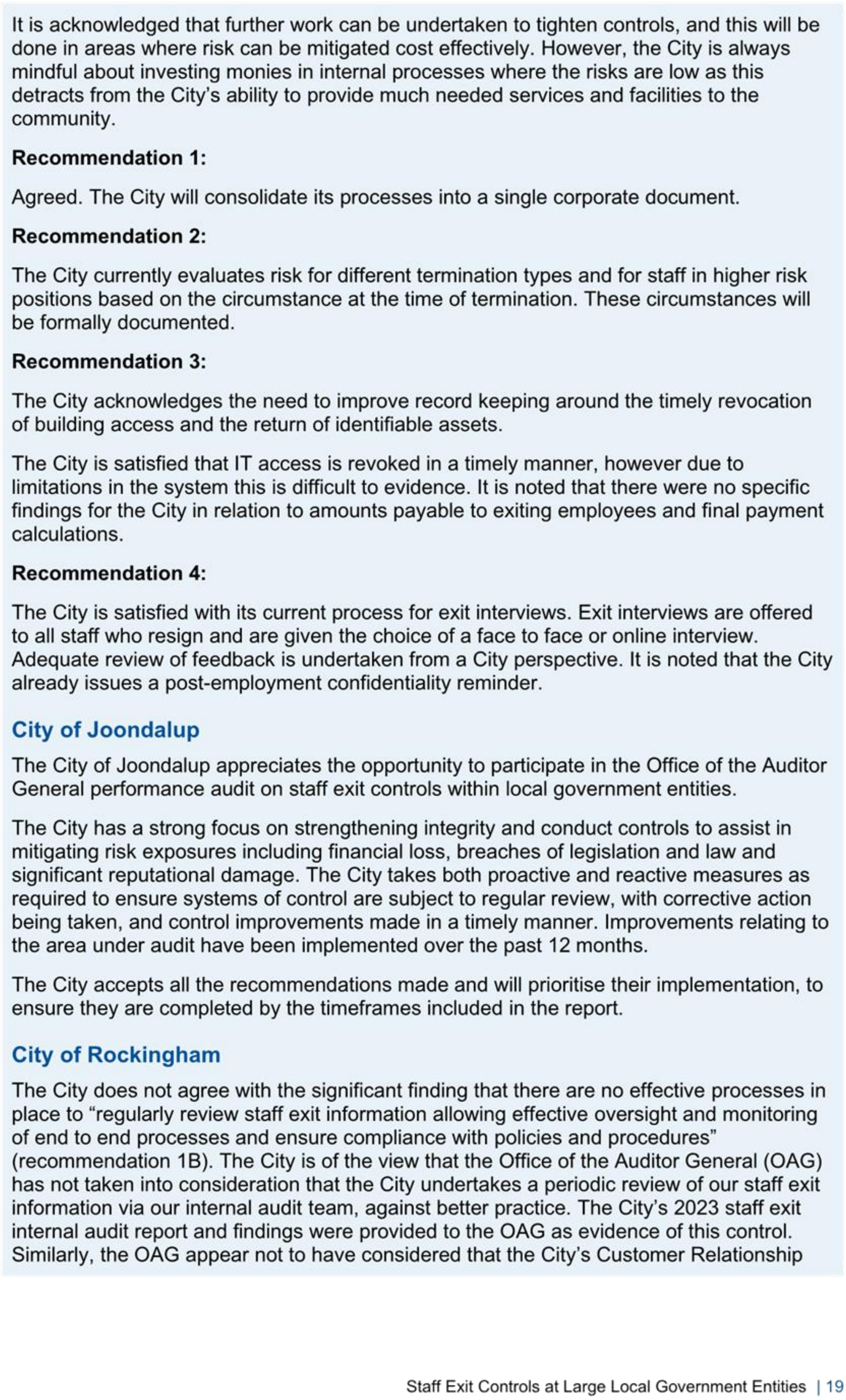
The City agrees with the findings and has a process in place for exit interviews. The requirement for post-employment confidentiality requirement confirmation processes will be built in the system for certain staff. The City does not agree with the implementation timeframe and the due date proposed to be set by the City is March 2025 to align with the implementation of the City's new ERP and the introduction of additional functionality for transitioning staff.

City of Canning

The City of Canning accepts the findings and welcomes the recommendations contained in the Summary of Findings report. It is pleasing that there was no evidence of loss or misuse and the City values the opportunity to focus on systemising practices to ensure risk is controlled.

City of Gosnells

It is very pleasing to note the audit found no instances where information systems were accessed inappropriately or where assets were lost or stolen. This would indicate that the controls in place are broadly effective and, consequently, the risk is low.



It is acknowledged that further work can be undertaken to tighten controls, and this will be done in areas where risk can be mitigated cost effectively. However, the City is always mindful about investing monies in internal processes where the risks are low as this detracts from the City's ability to provide much needed services and facilities to the community.

Recommendation 1:

Agreed. The City will consolidate its processes into a single corporate document.

Recommendation 2:

The City currently evaluates risk for different termination types and for staff in higher risk positions based on the circumstance at the time of termination. These circumstances will be formally documented.

Recommendation 3:

The City acknowledges the need to improve record keeping around the timely revocation of building access and the return of identifiable assets.

The City is satisfied that IT access is revoked in a timely manner, however due to limitations in the system this is difficult to evidence. It is noted that there were no specific findings for the City in relation to amounts payable to exiting employees and final payment calculations.

Recommendation 4:

The City is satisfied with its current process for exit interviews. Exit interviews are offered to all staff who resign and are given the choice of a face to face or online interview. Adequate review of feedback is undertaken from a City perspective. It is noted that the City already issues a post-employment confidentiality reminder.

City of Joondalup

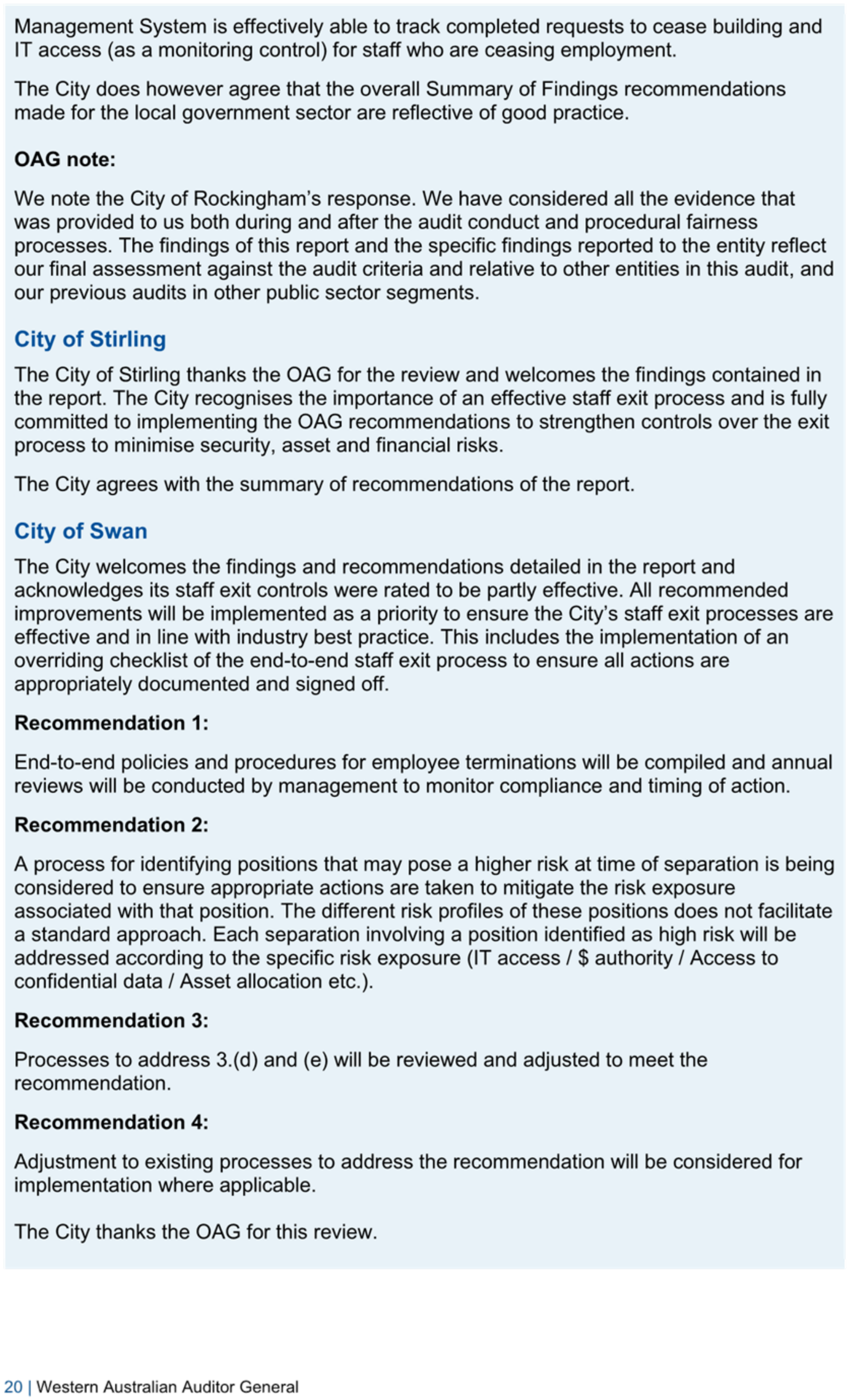
The City of Joondalup appreciates the opportunity to participate in the Office of the Auditor General performance audit on staff exit controls within local government entities.

The City has a strong focus on strengthening integrity and conduct controls to assist in mitigating risk exposures including financial loss, breaches of legislation and law and significant reputational damage. The City takes both proactive and reactive measures as required to ensure systems of control are subject to regular review, with corrective action being taken, and control improvements made in a timely manner. Improvements relating to the area under audit have been implemented over the past 12 months.

The City accepts all the recommendations made and will prioritise their implementation, to ensure they are completed by the timeframes included in the report.

City of Rockingham

The City does not agree with the significant finding that there are no effective processes in place to "regularly review staff exit information allowing effective oversight and monitoring of end to end processes and ensure compliance with policies and procedures" (recommendation 1B). The City is of the view that the Office of the Auditor General (OAG) has not taken into consideration that the City undertakes a periodic review of our staff exit information via our internal audit team, against better practice. The City's 2023 staff exit internal audit report and findings were provided to the OAG as evidence of this control. Similarly, the OAG appear not to have considered that the City's Customer Relationship



Management System is effectively able to track completed requests to cease building and IT access (as a monitoring control) for staff who are ceasing employment.

The City does however agree that the overall Summary of Findings recommendations made for the local government sector are reflective of good practice.

OAG note:

We note the City of Rockingham's response. We have considered all the evidence that was provided to us both during and after the audit conduct and procedural fairness processes. The findings of this report and the specific findings reported to the entity reflect our final assessment against the audit criteria and relative to other entities in this audit, and our previous audits in other public sector segments.

City of Stirling

The City of Stirling thanks the OAG for the review and welcomes the findings contained in the report. The City recognises the importance of an effective staff exit process and is fully committed to implementing the OAG recommendations to strengthen controls over the exit process to minimise security, asset and financial risks.

The City agrees with the summary of recommendations of the report.

City of Swan

The City welcomes the findings and recommendations detailed in the report and acknowledges its staff exit controls were rated to be partly effective. All recommended improvements will be implemented as a priority to ensure the City's staff exit processes are effective and in line with industry best practice. This includes the implementation of an overriding checklist of the end-to-end staff exit process to ensure all actions are appropriately documented and signed off.

Recommendation 1:

End-to-end policies and procedures for employee terminations will be compiled and annual reviews will be conducted by management to monitor compliance and timing of action.

Recommendation 2:

A process for identifying positions that may pose a higher risk at time of separation is being considered to ensure appropriate actions are taken to mitigate the risk exposure associated with that position. The different risk profiles of these positions does not facilitate a standard approach. Each separation involving a position identified as high risk will be addressed according to the specific risk exposure (IT access / $ authority / Access to confidential data / Asset allocation etc.).

Recommendation 3:

Processes to address 3.(d) and (e) will be reviewed and adjusted to meet the recommendation.

Recommendation 4:

Adjustment to existing processes to address the recommendation will be considered for implementation where applicable.

The City thanks the OAG for this review.

City of Wanneroo

The City of Wanneroo thanks the OAG for their review and welcomes the findings and recommendations. The City is fully committed to implementing recommendations that will support and strengthen the existing exit process, and appreciates that some processes were found to be effective. The City considers that implementation will further reduce the risks associated with staff that leave the organisation, particularly where they hold roles of additional authority. The recommendations will be progressed within the committed timeframes.

The City supports the summary of recommendations of the report.

Audit focus and scope

The audit assessed whether eight large metropolitan local government entities effectively and efficiently manage the exit of staff to minimise security, asset and financial risks.

The criteria assessed were:

- Do large local government entities have appropriate policies and procedures to effectively manage staff exits?
- Do large local government entities comply with staff exit policies and procedures?

The audit included the following entities:

- City of Armadale
- City of Canning
- City of Gosnells
- City of Joondalup
- City of Rockingham
- City of Stirling
- City of Swan
- City of Wanneroo.

The audit covered the period 1 January 2023 to 31 December 2023.

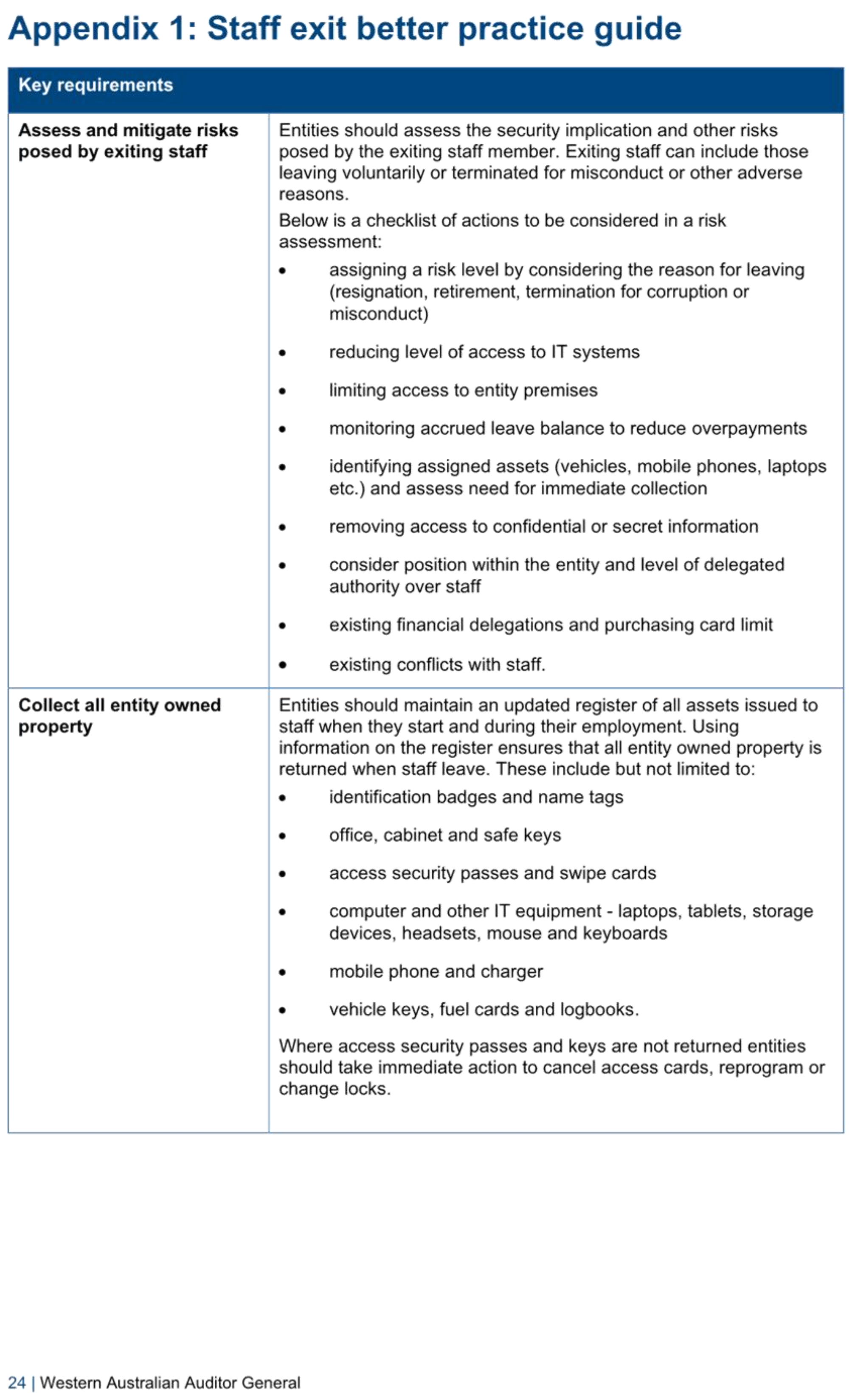
In conducting the audit we performed the following:

- held entrance meetings with the entities
- met with the Department of Local Government, Sport and Cultural Industries and local government sector bodies (Western Australian Local Government Association and Local Government Professionals WA)
- reviewed policy and procedure documents and supporting templates
- held meetings with key staff from human resources, payroll, finance, IT and security to gain an understanding of processes and perform walkthroughs
- tested a sample of 15 exits at each entity that covered positions of high level of responsibility or data access, field operatives and casual staff. This included 101, or 10% of, permanent staff and 19 casual staff
- sought evidence of exit processes:
    - termination checklists had been completed before or on the staff exit date and signed by the relevant authority
    - building access cards had been de-activated and/or keys had been collected prior to staff leaving
    - assets issued to staff (computers, tablets, mobile phones, vehicles) were returned
    - credit cards were returned and cancelled
    - access to the entity's IT systems was revoked within 24 hours of their departure

  - an exit interview was offered or conducted
  - final payments reviewed and money owed to the entity was identified and paid at the time of leaving
  - risks posed by departing staff and circumstances of their exit were assessed
- sought data on all exits to perform data analysis to assess the timeliness of the cancellation of IT and physical security access.

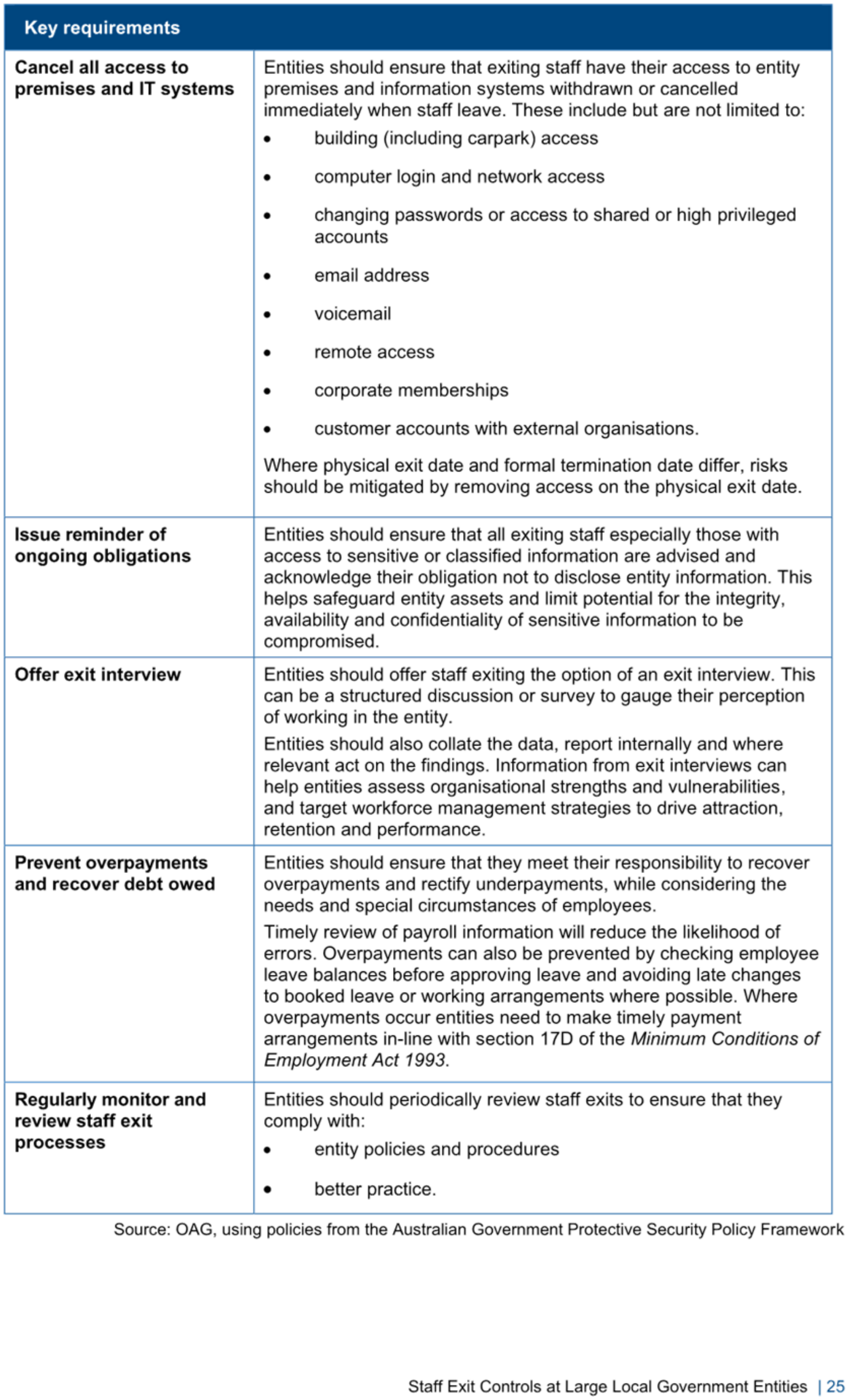
We did not assess termination decisions and whether they complied with the relevant legislation.

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 $285,000.



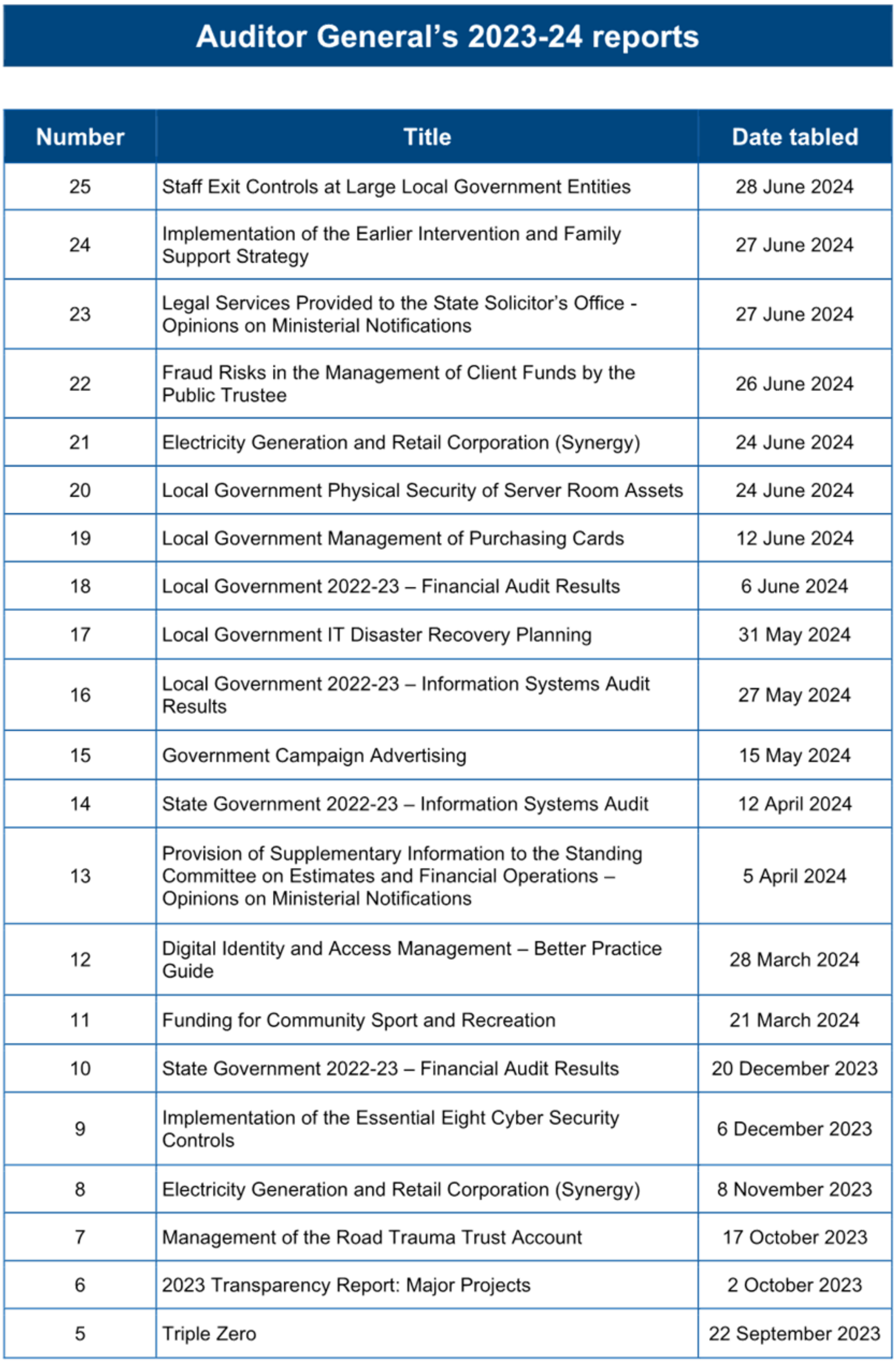
Appendix 1: Staff exit better practice guide

Key requirements	
Assess and mitigate risks posed by exiting staff	Entities should assess the security implication and other risks posed by the exiting staff member. Exiting staff can include those leaving voluntarily or terminated for misconduct or other adverse reasons. Below is a checklist of actions to be considered in a risk assessment: • assigning a risk level by considering the reason for leaving (resignation, retirement, termination for corruption or misconduct) • reducing level of access to IT systems • limiting access to entity premises • monitoring accrued leave balance to reduce overpayments • identifying assigned assets (vehicles, mobile phones, laptops etc.) and assess need for immediate collection • removing access to confidential or secret information • consider position within the entity and level of delegated authority over staff • existing financial delegations and purchasing card limit • existing conflicts with staff.
Collect all entity owned property	Entities should maintain an updated register of all assets issued to staff when they start and during their employment. Using information on the register ensures that all entity owned property is returned when staff leave. These include but not limited to: • identification badges and name tags • office, cabinet and safe keys • access security passes and swipe cards • computer and other IT equipment - laptops, tablets, storage devices, headsets, mouse and keyboards • mobile phone and charger • vehicle keys, fuel cards and logbooks. Where access security passes and keys are not returned entities should take immediate action to cancel access cards, reprogram or change locks.



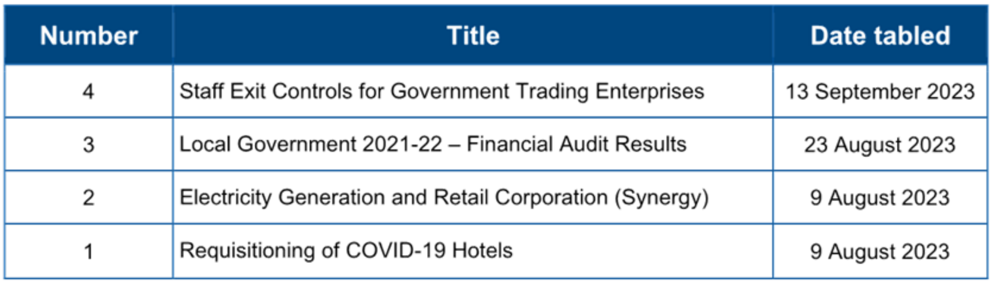
Key requirements	
Cancel all access to premises and IT systems	Entities should ensure that exiting staff have their access to entity premises and information systems withdrawn or cancelled immediately when staff leave. These include but are not limited to: • building (including carpark) access • computer login and network access • changing passwords or access to shared or high privileged accounts • email address • voicemail • remote access • corporate memberships • customer accounts with external organisations. Where physical exit date and formal termination date differ, risks should be mitigated by removing access on the physical exit date.
Issue reminder of ongoing obligations	Entities should ensure that all exiting staff especially those with access to sensitive or classified information are advised and acknowledge their obligation not to disclose entity information. This helps safeguard entity assets and limit potential for the integrity, availability and confidentiality of sensitive information to be compromised.
Offer exit interview	Entities should offer staff exiting the option of an exit interview. This can be a structured discussion or survey to gauge their perception of working in the entity. Entities should also collate the data, report internally and where relevant act on the findings. Information from exit interviews can help entities assess organisational strengths and vulnerabilities, and target workforce management strategies to drive attraction, retention and performance.
Prevent overpayments and recover debt owed	Entities should ensure that they meet their responsibility to recover overpayments and rectify underpayments, while considering the needs and special circumstances of employees. Timely review of payroll information will reduce the likelihood of errors. Overpayments can also be prevented by checking employee leave balances before approving leave and avoiding late changes to booked leave or working arrangements where possible. Where overpayments occur entities need to make timely payment arrangements in-line with section 17D of the *Minimum Conditions of Employment Act 1993*.
Regularly monitor and review staff exit processes	Entities should periodically review staff exits to ensure that they comply with: • entity policies and procedures • better practice.

Source: OAG, using policies from the Australian Government Protective Security Policy Framework



Auditor General’s 2023-24 reports

Number	Title	Date tabled
25	Staff Exit Controls at Large Local Government Entities	28 June 2024
24	Implementation of the Earlier Intervention and Family Support Strategy	27 June 2024
23	Legal Services Provided to the State Solicitor’s Office - Opinions on Ministerial Notifications	27 June 2024
22	Fraud Risks in the Management of Client Funds by the Public Trustee	26 June 2024
21	Electricity Generation and Retail Corporation (Synergy)	24 June 2024
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



Number	Title	Date tabled
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
for 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

Office of the Auditor General
Serving the Public Interest

Report 1: 2024-25 | 1 August 2024

BETTER PRACTICE GUIDE

Supplier Master Files

Office of the Auditor General
for Western Australia

Audit team:
Carl Huxtable
Forensic 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/Olivier Le Moal

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Supplier Master Files – Better Practice Guide

Report 1: 2024-25
1 August 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

SUPPLIER MASTER FILES – BETTER PRACTICE GUIDE

This report has been prepared for submission to Parliament under the provisions of sections 23 and 24 of the *Auditor General Act 2006*.

This better practice guide aims to help Western Australian (WA) public sector entities improve their management of supplier data. The guide focuses on better practices to reduce the risk of fraud and error in managing supplier data. It has been informed by my Office's examinations of supplier data management and input from WA public sector entities.

Caroline Spencer
Auditor General
1 August 2024

Contents

Auditor General's overview

From the smallest regional council to the largest state department, procurement of goods and services occurs daily in the Western Australian public sector. Vulnerabilities in poorly controlled and managed procurement systems and processes are prime targets for exploitation given the significant volume and value of financial transactions involved. It is therefore essential that these processes are designed and operated in ways that minimise the risks of fraud and corruption involving public money, as well as error.

Our financial and forensic audits across State and local government entities continue to identify shortfalls in the management of information about suppliers, including inadequate record keeping practices, and ineffective controls and weaknesses in data security. These shortfalls not only increase the risk of fraud and corruption occurring they also limit the ability to detect it.

Information about suppliers is a key part of the procurement process where problems can occur, and should be proactively managed rather than considered a static 'set and forget'. We encourage entities to examine systems, processes and controls relating to information about their suppliers to ensure accuracy and completeness as well as to prevent and even identify potential fraud. This guide aims to provide public sector entities with areas of focus to better create, manage and interrogate information about their suppliers to enhance their procurement process.

We acknowledge that each entity has its own level of maturity and capacity to implement the recommendations in this guide, whether due to system limitations or resource constraints. Nevertheless, we encourage entities to use this guide, along with additional resources to enhance their management of supplier information.

I thank the individuals from various public sector entities and professional firms who provided invaluable feedback to this guide.

Part 1: Introduction

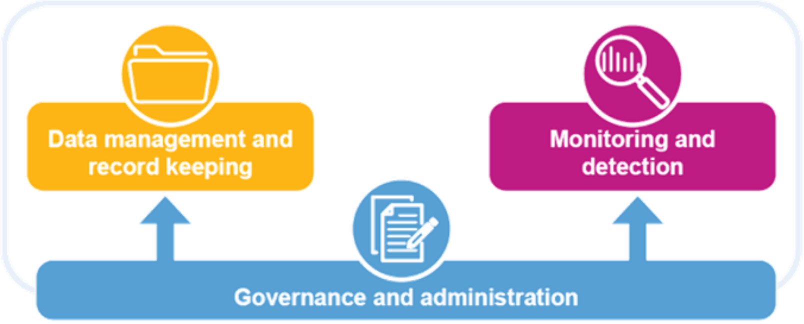
1.1 About this guide

This better practice guide aims to help Western Australian (WA) public sector entities to better structure, manage and interrogate supplier master files to support efficient and transparent procurement processes and reduce the risk of fraud and corruption, as well as error.

Our financial and forensic audits across State and local government entities continue to identify shortfalls in the management of supplier master data. Expanding on the findings and recommendations in our previous audit work[1], our Forensic Audit team recently completed a desktop analytics examination of supplier records from 10 WA public sector entities, each with between 416 and 211,129 individual supplier records.

The observations arising from our supplier data management examination and the feedback received from the participating entities have helped inform this better practice guide.

Part 2 of this guide sets out better practice for the management of supplier master data across three themes (Figure 1). The practical management of supplier master files needs to be underpinned by good governance and administration. These themes can be applied by entities in managing their supplier master data to reduce the risk of fraud or error.


Data management and record keeping
Monitoring and detection
Governance and administration

Source: OAG

Figure 1: Overview of better practice themes

While this guide is not intended to provide exhaustive guidance on broader procurement and supplier management practices and principles, we have included other matters to consider that may have a connection with how your supplier master data is managed.

Further guidance[2] is available through sources including:

- Public Sector Commission
- Department of Finance
- Department of Treasury
- Corruption and Crime Commission.

The term ‘supplier’ in this better practice guide is used to refer to both suppliers and vendors.

[1] Including Office of the Auditor General, *Management of Supplier Master Files*, OAG website, 7 March 2019.

[2] We have included a list of additional useful resources which have been prepared by these entities which may assist implementing or improving current supplier master data management practices (Appendix 3).

1.2 Who should use this guide

We encourage all public sector entities to consider the focus areas in this guide and how they may be best applied to managing supplier data as part of their entity's strong financial management.

In particular, this guide can benefit finance and accounting functions, including those who are owners of system design and implementation, within each entity.

Other business areas of the entity that may also have an interest include:

- procurement
- contract management
- risk and internal audit
- integrity and governance
- information and technology management.

1.3 Background

Procurement processes can be highly susceptible to several forms of fraud and corruption due to the involvement of various internal and external parties, and the significant volume and value of financial transactions involved.

Once supplier information is recorded in an entity's system, it is used for all future transactions and treated as correct. If this information is falsified, it can lead to fraudulent payments.

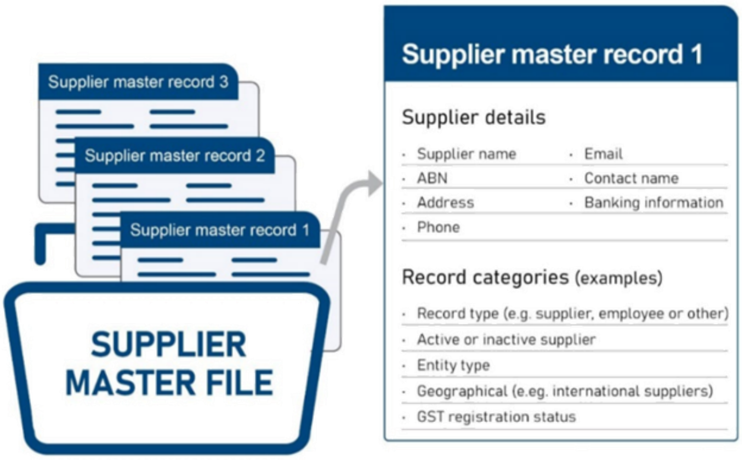
To mitigate this risk, entities should implement robust controls and procedures, conduct regular checks, and use technology and data analytics to detect errors, anomalies and suspicious patterns within procurement processes. External integrity or accountability bodies (including external audit) should not be seen as a replacement for robust internal controls and management oversight.

To support the principles in this guide and deter fraudulent activities, entities should foster a culture of integrity and ethical behaviour, promote reporting pathways including whistle-blower mechanisms, and provide training to employees on the requirements within procurement processes.

Supplier master information

A supplier master file is a centralised repository that contains important information about all suppliers to the entity, usually captured when onboarding a supplier as part of the procurement process.

Supplier master records are individual records within the supplier master file which relate to each specific supplier to the entity. Supplier master data refers to the actual data that has been collected in respect to each supplier that collectively comprises the supplier master record. Figure 2 details what a supplier master file contains.

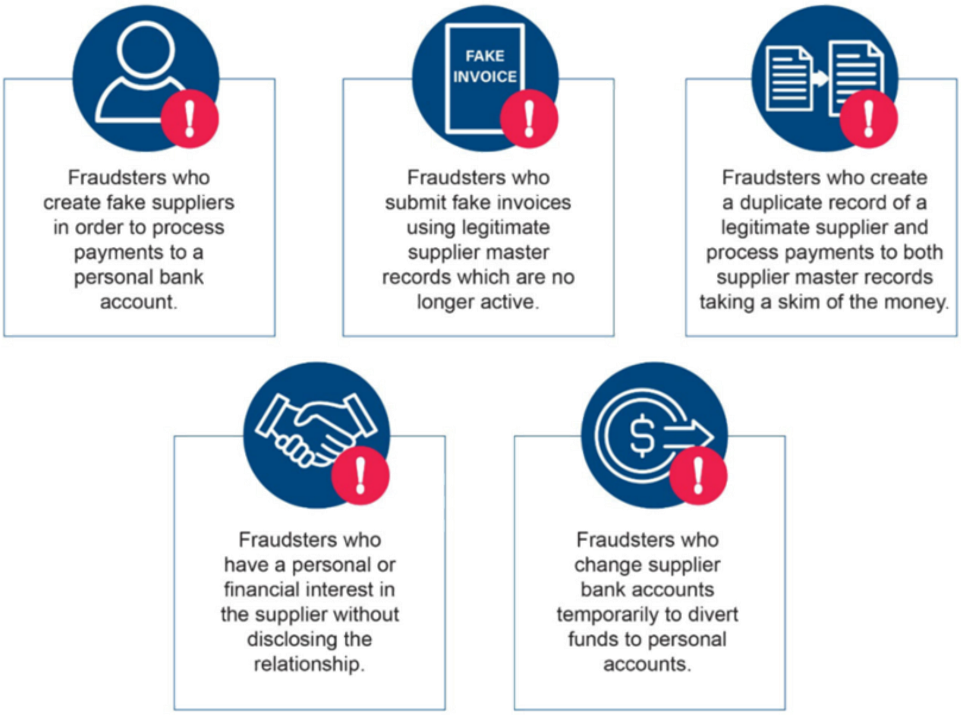


Source: OAG

Figure 2: Supplier master file and supplier master records

The supplier master file should serve as the single authoritative source for all supplier information and be subject to rigorous controls over the creation, amendment and use of the information recorded within it.

Supplier master data that is poorly managed may be exploited for fraudulent purposes, including:


FAKE INVOICE
Fraudsters who create fake suppliers in order to process payments to a personal bank account.
Fraudsters who submit fake invoices using legitimate supplier master records which are no longer active.
Fraudsters who create a duplicate record of a legitimate supplier and process payments to both supplier master records taking a skim of the money.
Fraudsters who have a personal or financial interest in the supplier without disclosing the relationship.
Fraudsters who change supplier bank accounts temporarily to divert funds to personal accounts.

Source: OAG

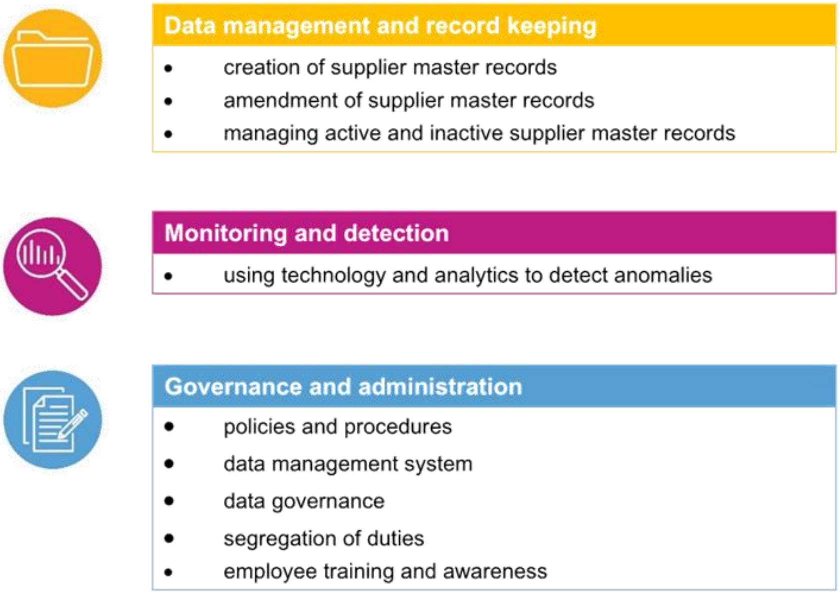
Figure 3: Common fraud scenarios in supplier data management

Part 2: Supplier data management better practice focus areas

The effective management of supplier master data is critical in protecting entities from the risk of error and fraud by ensuring the accuracy, completeness and legitimacy of information the entity holds about its suppliers.

This guide covers the key focus areas outlined in Figure 4 to help improve the WA public sector's practices in governing and managing supplier data.

We have included case studies to illustrate the risks and emphasise the importance of the better practice focus areas. These case studies are based on observations which arose during our supplier data management examination and other forensic audits conducted by our office.



Data management and record keeping

- creation of supplier master records
- amendment of supplier master records
- managing active and inactive supplier master records

Monitoring and detection

- using technology and analytics to detect anomalies

Governance and administration

- policies and procedures
- data management system
- data governance
- segregation of duties
- employee training and awareness

Source: OAG

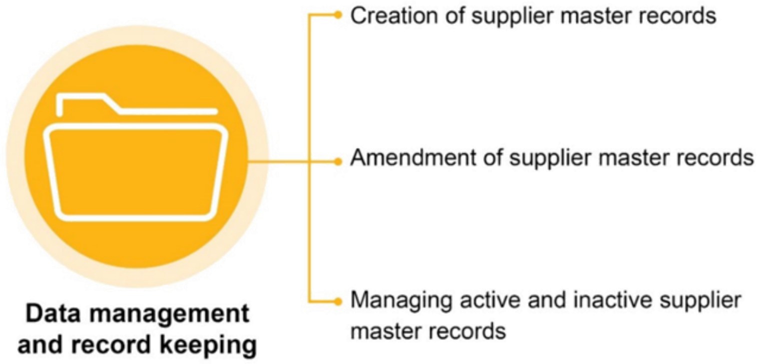
Figure 4: Overview of supplier data management focus areas

2.1 Data management and record keeping

When creating and amending supplier master records, entities should ensure that all supplier master data is accurate, complete, consistent and secure.

Entities should establish clear procedures which set out the process to be followed as well as templates which set out the detailed information required and relevant approvals for the creation and amendment of records.

Where possible, we encourage entities to automate these processes into its data management systems rather than relying on manual processes.


Creation of supplier master records
Amendment of supplier master records
Managing active and inactive supplier master records
Data management and record keeping

Source: OAG

Figure 5: Better practice themes in supplier data management and record keeping

2.1.1 Creation of supplier master records

When creating a new supplier master record, there are several steps which should be taken to ensure accuracy, completeness and consistency.

Gather information

Entities should gather all required information from each supplier to enable the accurate identification of the supplier and to conduct thorough due diligence enquiries (see 2.1.4) prior to creating a new supplier master record.

Supplier information that may be collected during onboarding to create a new supplier master record may include:

- business registration documents / details (and company details if relevant)
- contact information
- details of the goods and/or services that will be provided by the supplier
- banking and payment information
- the relevant terms and conditions that will apply to the engagement of that supplier.

Check that the supplier does not already exist in the system

Entities should establish procedures for verifying that a supplier has not already been recorded in the supplier master file prior to creating a new supplier master record to:

- avoid duplication, as this could result in data integrity issues, inefficiencies or the potential for exploitation and fraudulent activities

- ensure that payments are made to the correct entity and are able to be traced to a unique supplier master record
- improve visibility of spending and financial reporting across the entity's suppliers
- enable consistent and appropriate supplier relationship and communication
- provide clear audit trails of supplier transactions, interactions and compliance with internal policies and procedures.

Case study 1: Duplicate data identified in multiple supplier master records

Our supplier data management examination identified instances of supplier master records with duplicated information including:

- supplier name
- Australian Business Number (ABN)
- bank details
- contact information such as phone numbers or email addresses.

While there may be operational reasons for supplier master records to have duplicate data (for example, franchised entities which are separately operated), duplicate information may indicate:

- records which have been created in error or for fraudulent purposes. For example, fake supplier master records may be created to submit fraudulent invoices or divert payments to unauthorised accounts
- connections of interest between suppliers which may indicate potential collusion
- creation of additional supplier master records in order to subvert delegations of authority and split payment transactions.

We encourage entities to apply data flags to those supplier master records that have known and expected duplicate information (e.g. franchised entities). Entities should also conduct data matching analytics across the supplier master file to identify, investigate and resolve any supplier master records with duplicate information.

Classify record

Entities should identify relevant supplier classifications to be applied to each supplier master record. These classifications should be comprehensive enough to support the broader procurement process as well as aiding in conducting effective data analytics across supplier master data.

These classifications may include:

- clear identification of the record type: by classifying whether the record is a supplier, employee or other type of payee
- supplier activity status: this sets whether the record is active and able to be used for procurement purposes or is inactive
- geographical classification: this may include clearly identifying international suppliers to demonstrate why the data for these records is either not able to be obtained (e.g. Australian Business Number) or why the data is expected to be recorded in a different format (e.g. contact phone numbers)

- entity type: this may include applying a code to distinguish the type of supplier entity. For example, government, trusts, partnerships, private or public companies
- GST registration status: this identifies whether the supplier is registered for GST purposes.

Case study 2: Limited classification of supplier master records

Our supplier data management examination identified that many supplier master records were not classified in a manner that would enable clear identification of the record type or enable efficient and effective data driven detection analytics.

For example, many entities did not clearly identify and classify international suppliers. This presents challenges in being able to identify and separate those records which have legitimate incomplete data fields, such as an ABN.

This can result in an increased likelihood for false exceptions during data monitoring and detection procedures, and subsequent inefficiencies in identifying actual data integrity issues.

We encourage entities to apply relevant classifications to supplier master records which will enhance operational efficiency, improve data integrity and increase detection capabilities.

Test record creation process has worked

The supplier master record should be tested to ensure it functions correctly, captures all required information and follows the established policies and procedures.

The accuracy and completeness of the data entry should be checked for:

- typographical errors
- missing information
- inconsistencies that may affect data integrity, and which are not in line with the established data formats set by the entity.

All new records should be reviewed by an independent user (i.e. administrator) to ensure accuracy and legitimacy.

Activate the supplier master record

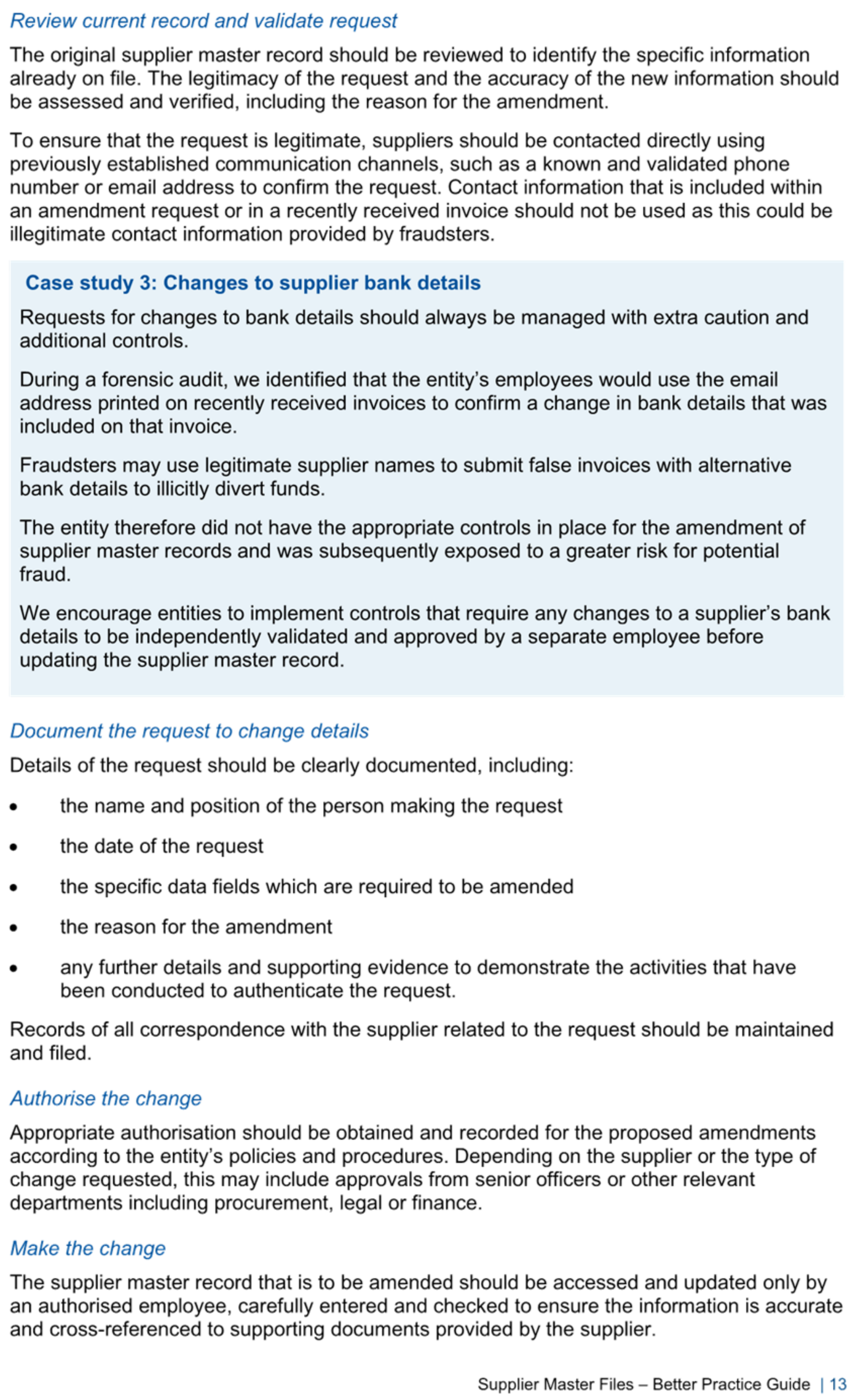
Supplier master records should only be activated in the supplier master file once all the required steps in the supplier onboarding, due diligence and data entry process have been completed and the supplier master record has been independently reviewed and approved.

These records may be referred to as needed during internal and external audits, compliance reviews or investigations.

2.1.2 Amendment of supplier master records

Requests to amend supplier master records may be received from a variety of sources. It is critical that any amendments made to supplier master records are independently validated and approved before being updated in the supplier master file.

When amending an existing supplier master record, there are several steps which should be taken to ensure that all amendments are handled securely, accurately and in compliance with relevant regulations and policies.



Review current record and validate request

The original supplier master record should be reviewed to identify the specific information already on file. The legitimacy of the request and the accuracy of the new information should be assessed and verified, including the reason for the amendment.

To ensure that the request is legitimate, suppliers should be contacted directly using previously established communication channels, such as a known and validated phone number or email address to confirm the request. Contact information that is included within an amendment request or in a recently received invoice should not be used as this could be illegitimate contact information provided by fraudsters.

Case study 3: Changes to supplier bank details

Requests for changes to bank details should always be managed with extra caution and additional controls.

During a forensic audit, we identified that the entity's employees would use the email address printed on recently received invoices to confirm a change in bank details that was included on that invoice.

Fraudsters may use legitimate supplier names to submit false invoices with alternative bank details to illicitly divert funds.

The entity therefore did not have the appropriate controls in place for the amendment of supplier master records and was subsequently exposed to a greater risk for potential fraud.

We encourage entities to implement controls that require any changes to a supplier's bank details to be independently validated and approved by a separate employee before updating the supplier master record.

Document the request to change details

Details of the request should be clearly documented, including:

- the name and position of the person making the request
- the date of the request
- the specific data fields which are required to be amended
- the reason for the amendment
- any further details and supporting evidence to demonstrate the activities that have been conducted to authenticate the request.

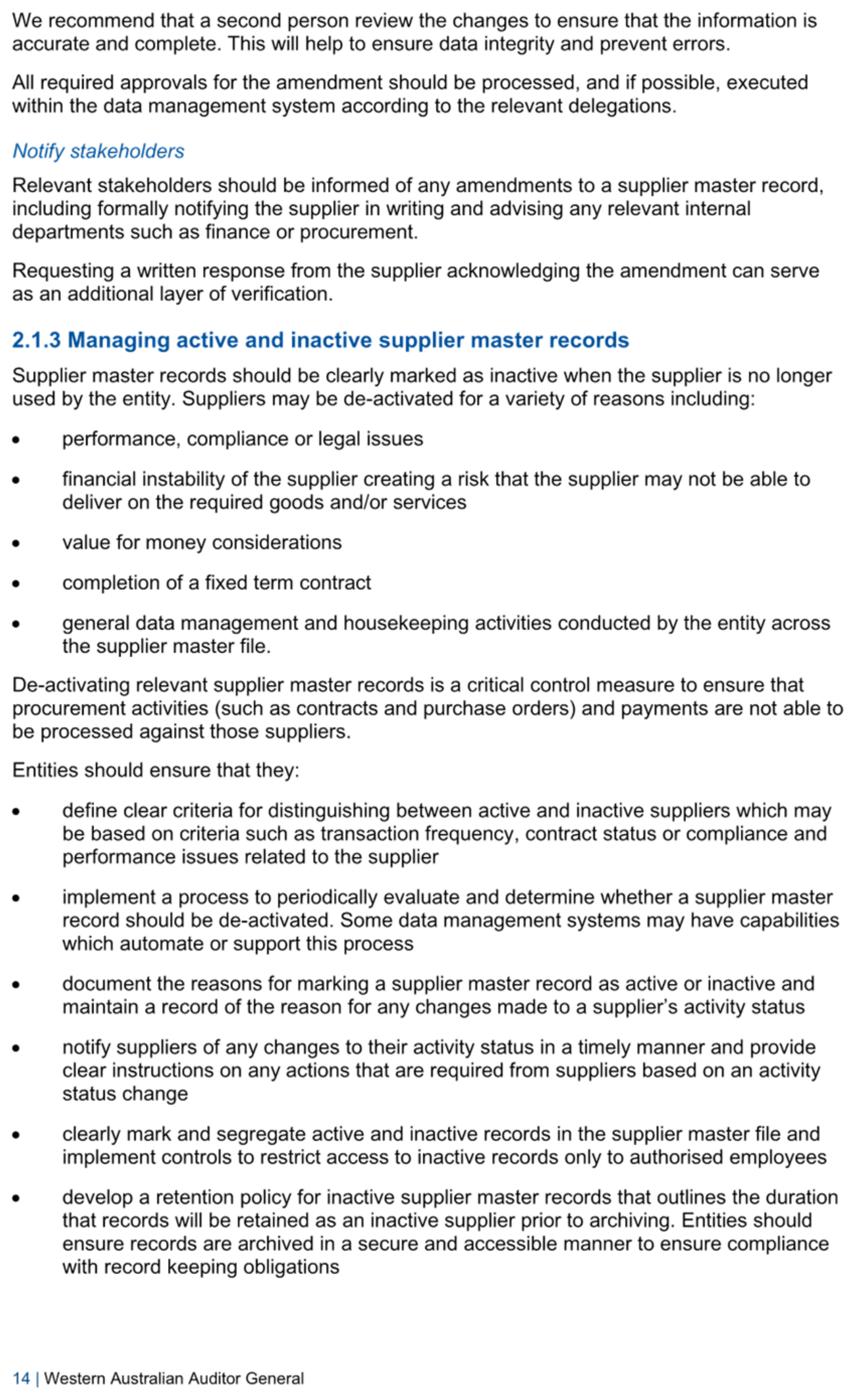
Records of all correspondence with the supplier related to the request should be maintained and filed.

Authorise the change

Appropriate authorisation should be obtained and recorded for the proposed amendments according to the entity's policies and procedures. Depending on the supplier or the type of change requested, this may include approvals from senior officers or other relevant departments including procurement, legal or finance.

Make the change

The supplier master record that is to be amended should be accessed and updated only by an authorised employee, carefully entered and checked to ensure the information is accurate and cross-referenced to supporting documents provided by the supplier.



We recommend that a second person review the changes to ensure that the information is accurate and complete. This will help to ensure data integrity and prevent errors.

All required approvals for the amendment should be processed, and if possible, executed within the data management system according to the relevant delegations.

Notify stakeholders

Relevant stakeholders should be informed of any amendments to a supplier master record, including formally notifying the supplier in writing and advising any relevant internal departments such as finance or procurement.

Requesting a written response from the supplier acknowledging the amendment can serve as an additional layer of verification.

2.1.3 Managing active and inactive supplier master records

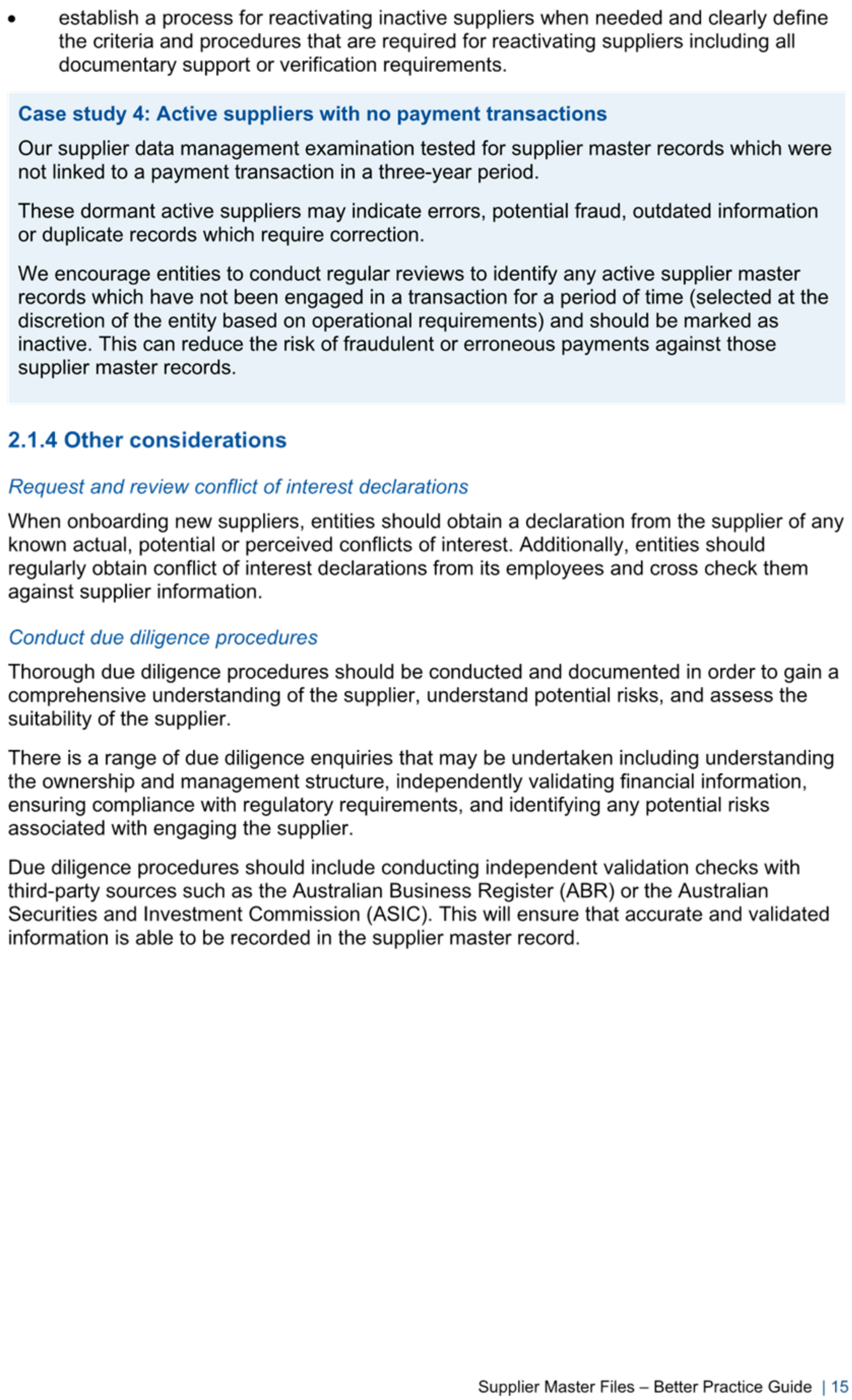
Supplier master records should be clearly marked as inactive when the supplier is no longer used by the entity. Suppliers may be de-activated for a variety of reasons including:

- performance, compliance or legal issues
- financial instability of the supplier creating a risk that the supplier may not be able to deliver on the required goods and/or services
- value for money considerations
- completion of a fixed term contract
- general data management and housekeeping activities conducted by the entity across the supplier master file.

De-activating relevant supplier master records is a critical control measure to ensure that procurement activities (such as contracts and purchase orders) and payments are not able to be processed against those suppliers.

Entities should ensure that they:

- define clear criteria for distinguishing between active and inactive suppliers which may be based on criteria such as transaction frequency, contract status or compliance and performance issues related to the supplier
- implement a process to periodically evaluate and determine whether a supplier master record should be de-activated. Some data management systems may have capabilities which automate or support this process
- document the reasons for marking a supplier master record as active or inactive and maintain a record of the reason for any changes made to a supplier's activity status
- notify suppliers of any changes to their activity status in a timely manner and provide clear instructions on any actions that are required from suppliers based on an activity status change
- clearly mark and segregate active and inactive records in the supplier master file and implement controls to restrict access to inactive records only to authorised employees
- develop a retention policy for inactive supplier master records that outlines the duration that records will be retained as an inactive supplier prior to archiving. Entities should ensure records are archived in a secure and accessible manner to ensure compliance with record keeping obligations



- establish a process for reactivating inactive suppliers when needed and clearly define the criteria and procedures that are required for reactivating suppliers including all documentary support or verification requirements.

Case study 4: Active suppliers with no payment transactions

Our supplier data management examination tested for supplier master records which were not linked to a payment transaction in a three-year period.

These dormant active suppliers may indicate errors, potential fraud, outdated information or duplicate records which require correction.

We encourage entities to conduct regular reviews to identify any active supplier master records which have not been engaged in a transaction for a period of time (selected at the discretion of the entity based on operational requirements) and should be marked as inactive. This can reduce the risk of fraudulent or erroneous payments against those supplier master records.

2.1.4 Other considerations

Request and review conflict of interest declarations

When onboarding new suppliers, entities should obtain a declaration from the supplier of any known actual, potential or perceived conflicts of interest. Additionally, entities should regularly obtain conflict of interest declarations from its employees and cross check them against supplier information.

Conduct due diligence procedures

Thorough due diligence procedures should be conducted and documented in order to gain a comprehensive understanding of the supplier, understand potential risks, and assess the suitability of the supplier.

There is a range of due diligence enquiries that may be undertaken including understanding the ownership and management structure, independently validating financial information, ensuring compliance with regulatory requirements, and identifying any potential risks associated with engaging the supplier.

Due diligence procedures should include conducting independent validation checks with third-party sources such as the Australian Business Register (ABR) or the Australian Securities and Investment Commission (ASIC). This will ensure that accurate and validated information is able to be recorded in the supplier master record.

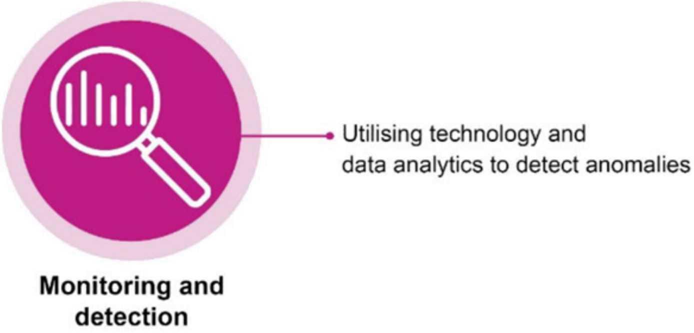
2.2 Monitoring and detection

As part of fraud detection activities, entities should establish routine processes to monitor controls and detect potential anomalies in supplier master files through the use of data analytics.

Regular examination of supplier master data should be conducted to ensure:

- activities that are being conducted by employees are in compliance with relevant policies, procedures and controls
- new records or amendments are appropriately supported and approved
- supplier master data is accurate, complete and consistent
- anomalies are identified and examined in a timely manner.

Employees who perform monitoring and detection activities should not be the same employees who are responsible for managing supplier master data. Segregating these duties will provide for independence in the review process.



Source: OAG

Figure 6: Better practice in monitoring and detection

2.2.1 Utilising technology and data analytics to detect anomalies

Data driven detection analytics involves collecting and analysing a variety of relevant internal and external data sources to produce information in a format that allows for a timely response or investigation and can be regularly repeated to check for unexpected changes and patterns.

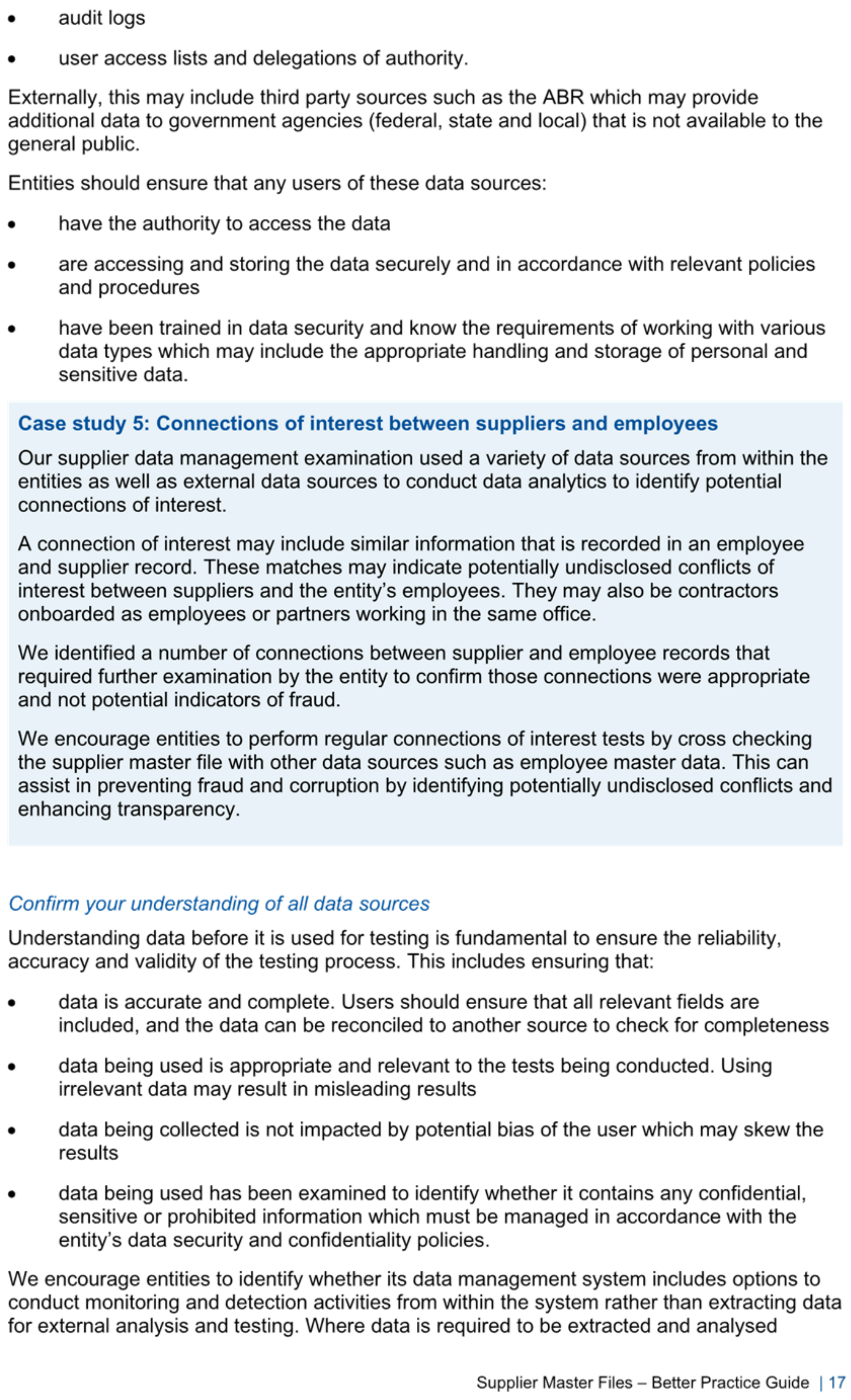
Entities should explore the use of various technology options for analysing supplier master data including data analytics, artificial intelligence, and automated detection tools.

When conducting data driven detection analytics in supplier data management, there are several steps which should be taken to ensure that the source data can be relied on and effectively used for analysis.

Identify relevant data sources

Entities should identify the various data sources that are relevant and available to conduct data driven detection analytics in respect of supplier activity. Internally, this may include:

- supplier master file data
- supplier payments data
- employee data



- audit logs
- user access lists and delegations of authority.

Externally, this may include third party sources such as the ABR which may provide additional data to government agencies (federal, state and local) that is not available to the general public.

Entities should ensure that any users of these data sources:

- have the authority to access the data
- are accessing and storing the data securely and in accordance with relevant policies and procedures
- have been trained in data security and know the requirements of working with various data types which may include the appropriate handling and storage of personal and sensitive data.

Case study 5: Connections of interest between suppliers and employees

Our supplier data management examination used a variety of data sources from within the entities as well as external data sources to conduct data analytics to identify potential connections of interest.

A connection of interest may include similar information that is recorded in an employee and supplier record. These matches may indicate potentially undisclosed conflicts of interest between suppliers and the entity's employees. They may also be contractors onboarded as employees or partners working in the same office.

We identified a number of connections between supplier and employee records that required further examination by the entity to confirm those connections were appropriate and not potential indicators of fraud.

We encourage entities to perform regular connections of interest tests by cross checking the supplier master file with other data sources such as employee master data. This can assist in preventing fraud and corruption by identifying potentially undisclosed conflicts and enhancing transparency.

Confirm your understanding of all data sources

Understanding data before it is used for testing is fundamental to ensure the reliability, accuracy and validity of the testing process. This includes ensuring that:

- data is accurate and complete. Users should ensure that all relevant fields are included, and the data can be reconciled to another source to check for completeness
- data being used is appropriate and relevant to the tests being conducted. Using irrelevant data may result in misleading results
- data being collected is not impacted by potential bias of the user which may skew the results
- data being used has been examined to identify whether it contains any confidential, sensitive or prohibited information which must be managed in accordance with the entity's data security and confidentiality policies.

We encourage entities to identify whether its data management system includes options to conduct monitoring and detection activities from within the system rather than extracting data for external analysis and testing. Where data is required to be extracted and analysed external to the system, entities should ensure that this is conducted in a secure data environment and is only accessible by authorised employees.

Prepare data for analysis

Data should be prepared, cleansed and structured before analysis to ensure the accuracy, reliability, and effectiveness of the analysis process.

Data preparation procedures may include:

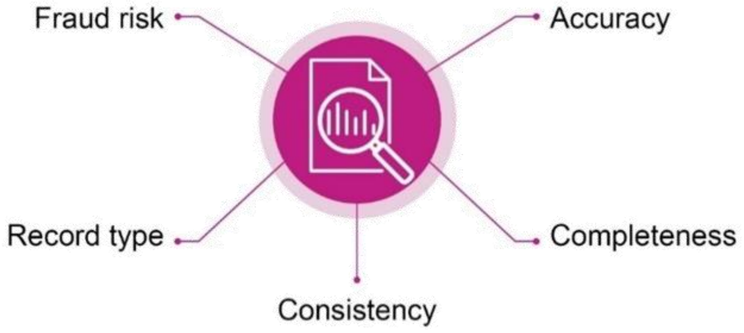
- identifying missing data
- managing duplicate data
- standardising data to ensure consistent formats across data fields
- correcting errors
- identifying and managing outliers which could skew analysis results
- removing irrelevant data
- performing checks to ensure data integrity and conducting quality review.

Conducting data analytics tests for monitoring and detection

To ensure the accuracy, completeness and consistency of supplier master data, and to check for potential fraud or error, there are various tests which can be conducted by entities using a data driven analytics approach.

Any anomalies that arise from data analytics tests or analysis should be examined first to understand the reason why – for example is there an operational reason, data entry error or potential fraud requiring further investigation.

We provide at Appendix 2 a list of example data analytics tests that can be conducted by entities.



Source: OAG

Figure 7: Data analytics testing themes

2.2.2 Other considerations

Post detection and reporting activities

Control weaknesses or supplier master data anomalies that have been identified from monitoring and detection activities should be explored to understand what further steps need to be taken. This may include applying corrective actions to mitigate risks, conducting detailed investigation or initiating formal reporting.

Additional information should be obtained about the weaknesses or anomalies that have been identified including:

- understanding the potential impact of the issue
- identifying the potential risks that may arise from the issue and conducting a risk assessment
- identifying the types of activities or transactions which may have been compromised or impacted
- the extent of the current and potential impact of the issue
- individuals that are involved in or connected to the issue
- the potential cause which may include human error, fraud or system vulnerabilities
- other data or information which is available and may be relevant to examining the matter.

Investigate and report

If further investigation is required, entities should seek to understand whether they have the appropriate internal capacity, capabilities and independence to investigate. Alternatively, entities may seek to engage a third party to conduct detailed investigations.

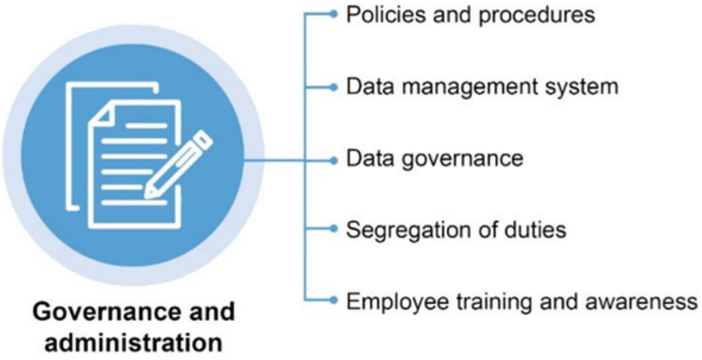
Findings which arise from internal audits or monitoring and detection activities should be reported to the entity's audit and risk committee, and clearly set out the areas of concern, recommendations and action plan.

Where there is a reasonable suspicion of misconduct, public sector entities are required to report minor misconduct matters to the Public Sector Commission (PSC) and serious misconduct matters to the Corruption and Crime Commission (CCC).

2.3 Governance and administration

The practical management of supplier master files needs to be underpinned by good governance and administration. Governance frameworks outline the policies, procedures, roles and responsibilities that are required to effectively manage an entity's operations in a transparent, accountable and efficient manner.

It is crucial that appropriate guidance for the effective management of supplier master files is incorporated into the entity's broader governance framework to ensure that supplier master data is managed appropriately.



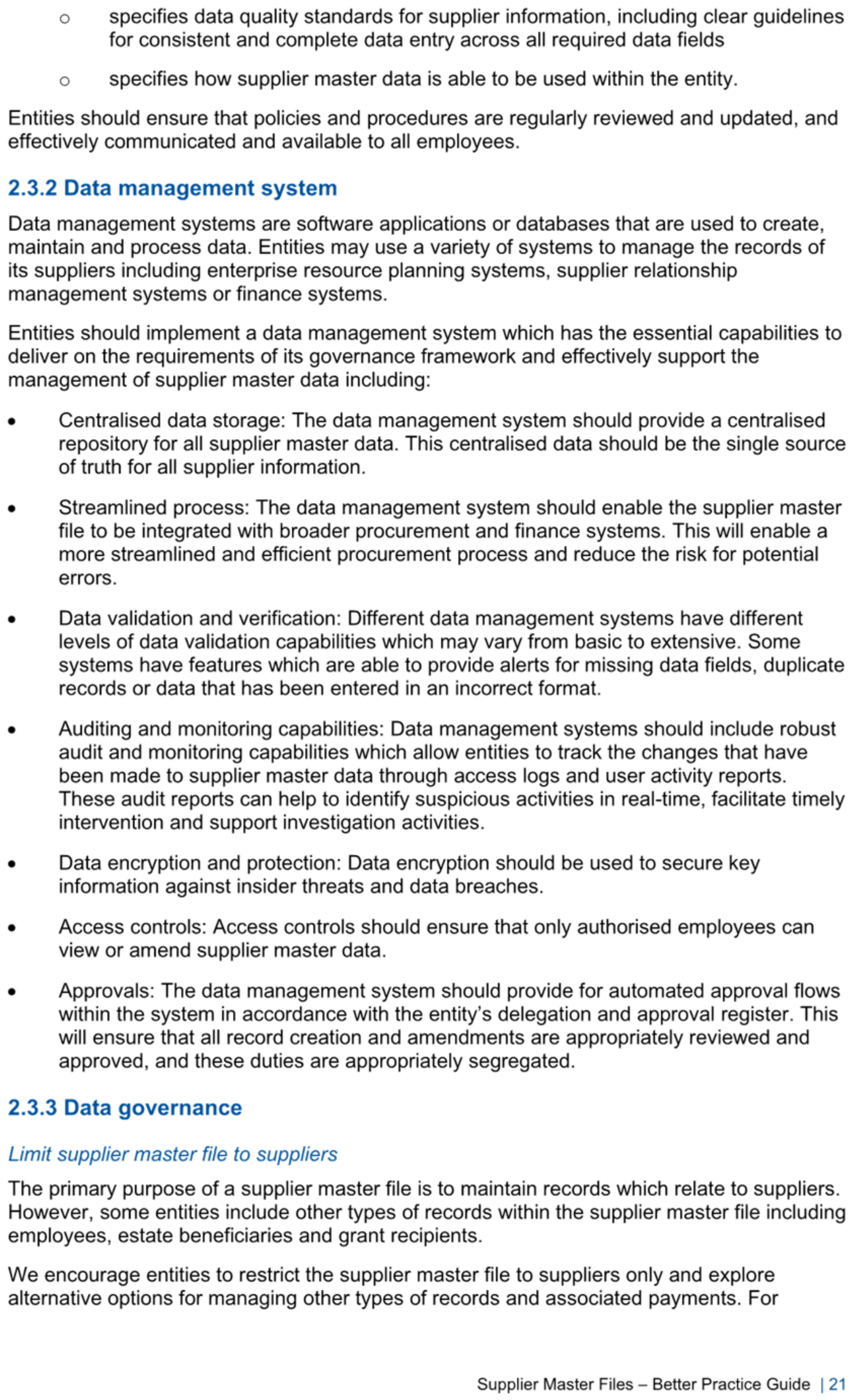
Source: OAG

Figure 8: Better practice focus areas for supplier master file governance and administration

2.3.1 Policies and procedures

In ensuring there is clear governance and administration in place to structure, manage and interrogate supplier master files, key processes should be formalised within policies and procedures, such as:

- Supplier onboarding:
  - defines the criteria and procedures for onboarding new suppliers
  - specifies the documentation that is required to be collected from suppliers to support the data entered into the supplier master record
  - establishes a guide for managing relationships with suppliers including approved communication methods.
- Supplier data management:
  - defines the purpose and scope of the supplier master file, including the type of records that are approved to be included
  - outlines the role of the supplier master file in the broader procurement process
  - establishes the procedures required for creating, amending and maintaining supplier master records to ensure accuracy, completeness and consistency in the data entry process
  - outlines the roles, responsibilities, authorisation and access for employees who create, amend, approve and manage supplier master records



- specifies data quality standards for supplier information, including clear guidelines for consistent and complete data entry across all required data fields
- specifies how supplier master data is able to be used within the entity.

Entities should ensure that policies and procedures are regularly reviewed and updated, and effectively communicated and available to all employees.

2.3.2 Data management system

Data management systems are software applications or databases that are used to create, maintain and process data. Entities may use a variety of systems to manage the records of its suppliers including enterprise resource planning systems, supplier relationship management systems or finance systems.

Entities should implement a data management system which has the essential capabilities to deliver on the requirements of its governance framework and effectively support the management of supplier master data including:

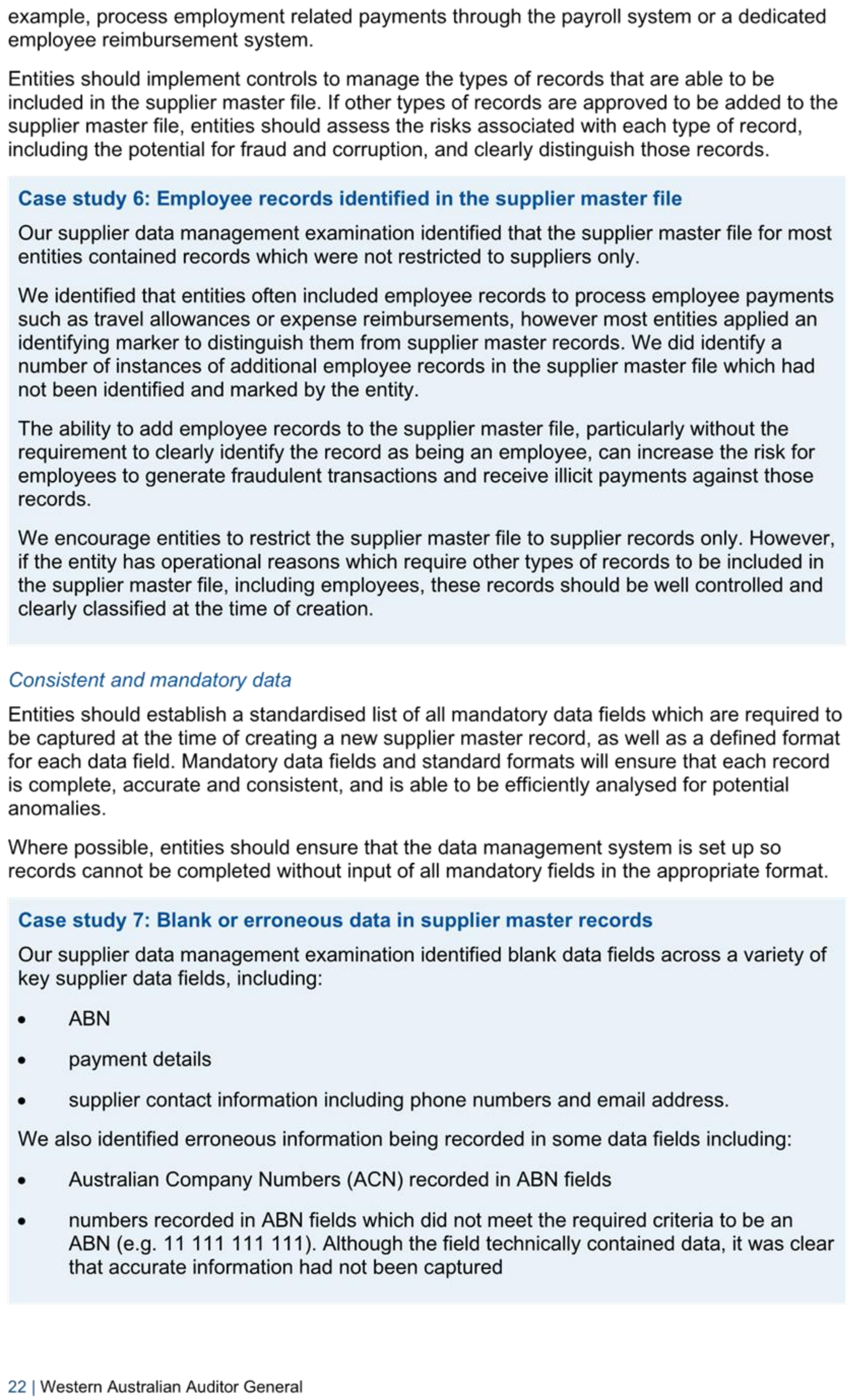
- Centralised data storage: The data management system should provide a centralised repository for all supplier master data. This centralised data should be the single source of truth for all supplier information.
- Streamlined process: The data management system should enable the supplier master file to be integrated with broader procurement and finance systems. This will enable a more streamlined and efficient procurement process and reduce the risk for potential errors.
- Data validation and verification: Different data management systems have different levels of data validation capabilities which may vary from basic to extensive. Some systems have features which are able to provide alerts for missing data fields, duplicate records or data that has been entered in an incorrect format.
- Auditing and monitoring capabilities: Data management systems should include robust audit and monitoring capabilities which allow entities to track the changes that have been made to supplier master data through access logs and user activity reports. These audit reports can help to identify suspicious activities in real-time, facilitate timely intervention and support investigation activities.
- Data encryption and protection: Data encryption should be used to secure key information against insider threats and data breaches.
- Access controls: Access controls should ensure that only authorised employees can view or amend supplier master data.
- Approvals: The data management system should provide for automated approval flows within the system in accordance with the entity's delegation and approval register. This will ensure that all record creation and amendments are appropriately reviewed and approved, and these duties are appropriately segregated.

2.3.3 Data governance

Limit supplier master file to suppliers

The primary purpose of a supplier master file is to maintain records which relate to suppliers. However, some entities include other types of records within the supplier master file including employees, estate beneficiaries and grant recipients.

We encourage entities to restrict the supplier master file to suppliers only and explore alternative options for managing other types of records and associated payments. For



example, process employment related payments through the payroll system or a dedicated employee reimbursement system.

Entities should implement controls to manage the types of records that are able to be included in the supplier master file. If other types of records are approved to be added to the supplier master file, entities should assess the risks associated with each type of record, including the potential for fraud and corruption, and clearly distinguish those records.

Case study 6: Employee records identified in the supplier master file

Our supplier data management examination identified that the supplier master file for most entities contained records which were not restricted to suppliers only.

We identified that entities often included employee records to process employee payments such as travel allowances or expense reimbursements, however most entities applied an identifying marker to distinguish them from supplier master records. We did identify a number of instances of additional employee records in the supplier master file which had not been identified and marked by the entity.

The ability to add employee records to the supplier master file, particularly without the requirement to clearly identify the record as being an employee, can increase the risk for employees to generate fraudulent transactions and receive illicit payments against those records.

We encourage entities to restrict the supplier master file to supplier records only. However, if the entity has operational reasons which require other types of records to be included in the supplier master file, including employees, these records should be well controlled and clearly classified at the time of creation.

Consistent and mandatory data

Entities should establish a standardised list of all mandatory data fields which are required to be captured at the time of creating a new supplier master record, as well as a defined format for each data field. Mandatory data fields and standard formats will ensure that each record is complete, accurate and consistent, and is able to be efficiently analysed for potential anomalies.

Where possible, entities should ensure that the data management system is set up so records cannot be completed without input of all mandatory fields in the appropriate format.

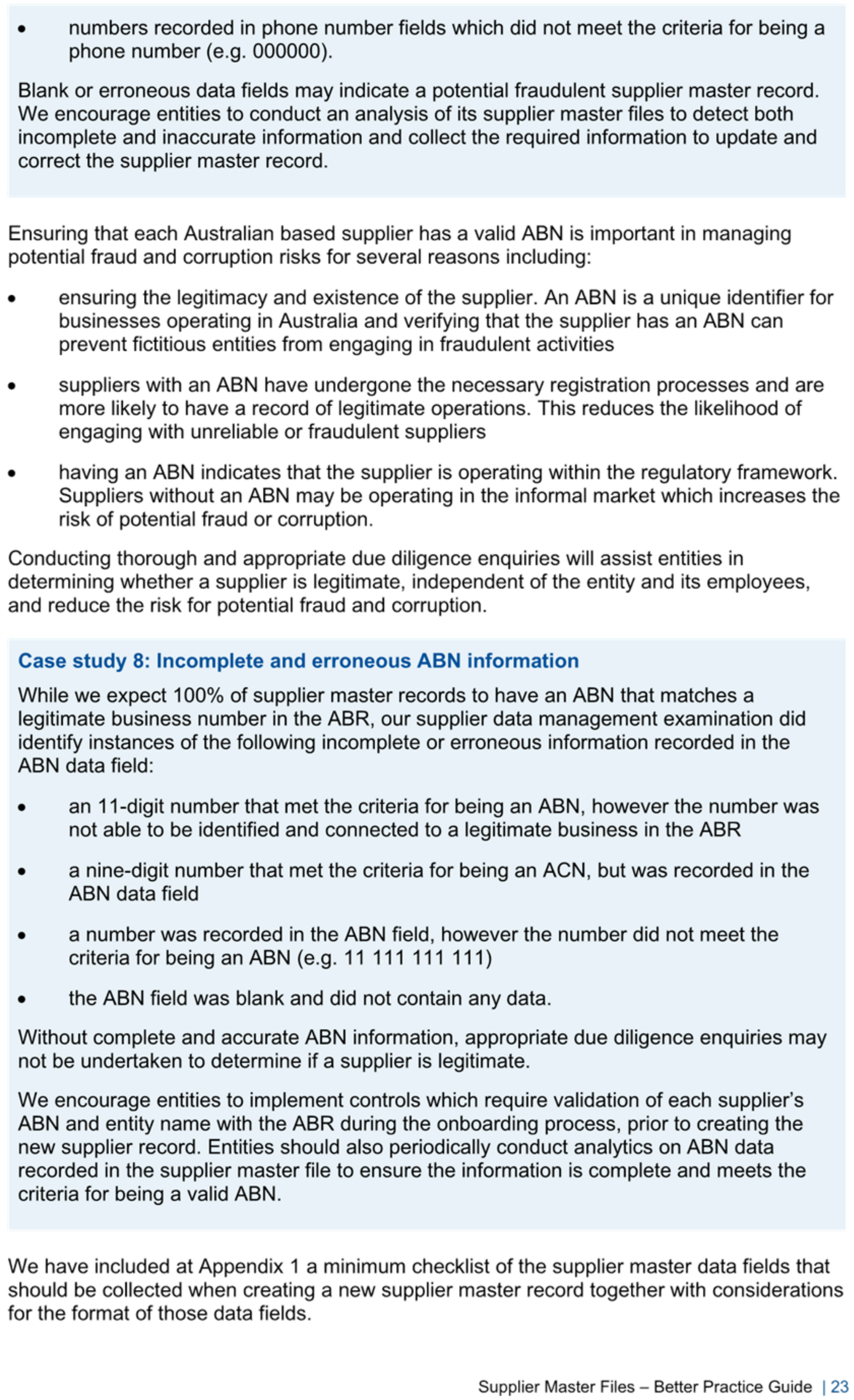
Case study 7: Blank or erroneous data in supplier master records

Our supplier data management examination identified blank data fields across a variety of key supplier data fields, including:

- ABN
- payment details
- supplier contact information including phone numbers and email address.

We also identified erroneous information being recorded in some data fields including:

- Australian Company Numbers (ACN) recorded in ABN fields
- numbers recorded in ABN fields which did not meet the required criteria to be an ABN (e.g. 11 111 111 111). Although the field technically contained data, it was clear that accurate information had not been captured



- numbers recorded in phone number fields which did not meet the criteria for being a phone number (e.g. 000000).

Blank or erroneous data fields may indicate a potential fraudulent supplier master record. We encourage entities to conduct an analysis of its supplier master files to detect both incomplete and inaccurate information and collect the required information to update and correct the supplier master record.

Ensuring that each Australian based supplier has a valid ABN is important in managing potential fraud and corruption risks for several reasons including:

- ensuring the legitimacy and existence of the supplier. An ABN is a unique identifier for businesses operating in Australia and verifying that the supplier has an ABN can prevent fictitious entities from engaging in fraudulent activities
- suppliers with an ABN have undergone the necessary registration processes and are more likely to have a record of legitimate operations. This reduces the likelihood of engaging with unreliable or fraudulent suppliers
- having an ABN indicates that the supplier is operating within the regulatory framework. Suppliers without an ABN may be operating in the informal market which increases the risk of potential fraud or corruption.

Conducting thorough and appropriate due diligence enquiries will assist entities in determining whether a supplier is legitimate, independent of the entity and its employees, and reduce the risk for potential fraud and corruption.

Case study 8: Incomplete and erroneous ABN information

While we expect 100% of supplier master records to have an ABN that matches a legitimate business number in the ABR, our supplier data management examination did identify instances of the following incomplete or erroneous information recorded in the ABN data field:

- an 11-digit number that met the criteria for being an ABN, however the number was not able to be identified and connected to a legitimate business in the ABR
- a nine-digit number that met the criteria for being an ACN, but was recorded in the ABN data field
- a number was recorded in the ABN field, however the number did not meet the criteria for being an ABN (e.g. 11 111 111 111)
- the ABN field was blank and did not contain any data.

Without complete and accurate ABN information, appropriate due diligence enquiries may not be undertaken to determine if a supplier is legitimate.

We encourage entities to implement controls which require validation of each supplier’s ABN and entity name with the ABR during the onboarding process, prior to creating the new supplier record. Entities should also periodically conduct analytics on ABN data recorded in the supplier master file to ensure the information is complete and meets the criteria for being a valid ABN.

We have included at Appendix 1 a minimum checklist of the supplier master data fields that should be collected when creating a new supplier master record together with considerations for the format of those data fields.

2.3.4 Segregation of duties

Segregation of duties within the supplier data management process is essential to ensure integrity and transparency and reduce the risk for potential errors and fraud.

Entities should implement effective internal controls to ensure that there is an appropriate segregation of duties which may include:

- the creation of new supplier master records or amendments to existing records, requiring independent validation and approval by a second employee
- employees who create or amend supplier master records are not authorised to process an invoice or approve payment for that supplier.

When it is not possible to segregate duties (for example, within small entities that have a limited number of employees), entities should report the limitations to the entity's audit and risk committee and implement other compensating controls to mitigate key areas of risk.

Where possible, entities should ensure that data management systems are set up to apply any relevant internal controls and the required segregation of duties.

2.3.5 Employee training and awareness

All employees should be provided with training relevant to their role. Employees with responsibilities relating to supplier master files should understand the important role this information plays in the procurement process and the potential consequences of non-compliance with policy and process.

Key training themes should encompass data accuracy and integrity, compliance with governance requirements, proficiency in relevant systems and data security. Additionally, employees should be educated on potential fraud risks in supplier data management and the available mechanisms for reporting such issues.

2.3.6 Other considerations

In addition to the above governance and administrations processes, we have set out related areas that entities may consider in their supplier data management process.

Policies and procedures

- Procurement – supplier master data is treated as being 'true' when purchasing, receipting and paying for goods and services, therefore all procurement processes should consider how they interact and cross reference where appropriate. It is also essential that all employees with responsibilities relating to supplier master data are aware of their obligations around data security and common types of fraud and corruption that may arise in supplier data management.
- Security and confidentiality of records – requirements and procedures for handling of sensitive, restricted or prohibited information, encryption requirements for data storage and transfer, and measures to prevent data breaches and cyber attacks.
- Conflicts of interest – employees with responsibilities relating to supplier master data should be aware of their obligations to declare actual, potential or perceived conflicts of interest as they arise and abstain from the management of supplier master records where they have declared a conflict of interest. Employees should also appreciate how incomplete or inaccurate data management prevents the identification of undisclosed relationships.

- Data retention and disposal – each entity will have a record keeping plan, which will incorporate how records[3] are managed for retention and destruction.
- Audit and compliance – the entity outlines procedures for conducting internal audits, and compliance and risk assessments relating to supplier master records and measures for addressing non-compliance.
- Whistleblower or public interest disclosure – the entity documents the process to be taken in reporting suspected unethical behaviour or conflicts of interest.

Risk identification and assessment

Entities should appropriately analyse, evaluate and mitigate risks.

Risks connected to supplier data management may be identified across the following areas:

- data integrity and accuracy
- compliance with regulations
- accountability and transparency
- confidentiality and security of data
- fraud and corruption
- operational efficiencies
- conflicts of interest.

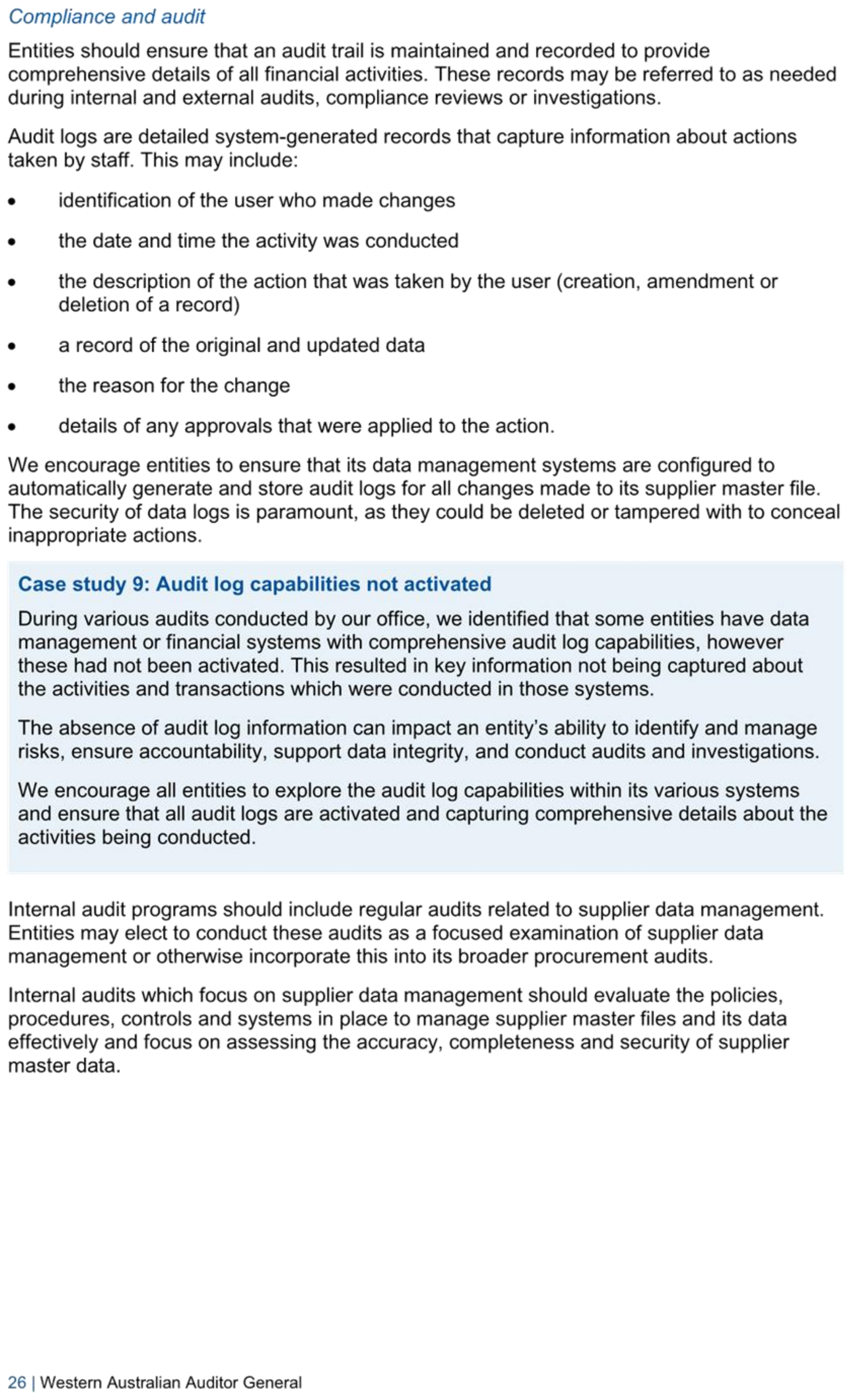
Training

Training should be delivered regularly to ensure that employees remain informed about the entity's policies and procedures, best practice and any emerging risks. Training schedules may include:

- Initial training: New employees should be provided training as part of the onboarding process. This will ensure they understand the entity's policies and procedures, data management system and the importance of effective supplier data management from the beginning.
- Annual refresher: Employees should complete annual refresher training to reinforce key concepts and update them on any changes to policies and procedures.
- Periodic updates: Training should be conducted at any time there is substantial changes to policies, procedures or regulatory requirements.
- Reactive: Training should be provided following any incidents or audit findings to prevent similar events happening in the future, and to ensure continuous improvement and risk mitigation.

Training can be delivered to employees through a variety of methods including workshops, online courses or through the use of guidance documents and manuals. In larger entities, the content and frequency of training may need to be tailored for the various cohorts of employees with different roles and responsibilities in supplier data management.

[3] section 3(1) of the *State Records Act 2000* (WA)



Compliance and audit

Entities should ensure that an audit trail is maintained and recorded to provide comprehensive details of all financial activities. These records may be referred to as needed during internal and external audits, compliance reviews or investigations.

Audit logs are detailed system-generated records that capture information about actions taken by staff. This may include:

- identification of the user who made changes
- the date and time the activity was conducted
- the description of the action that was taken by the user (creation, amendment or deletion of a record)
- a record of the original and updated data
- the reason for the change
- details of any approvals that were applied to the action.

We encourage entities to ensure that its data management systems are configured to automatically generate and store audit logs for all changes made to its supplier master file. The security of data logs is paramount, as they could be deleted or tampered with to conceal inappropriate actions.

Case study 9: Audit log capabilities not activated

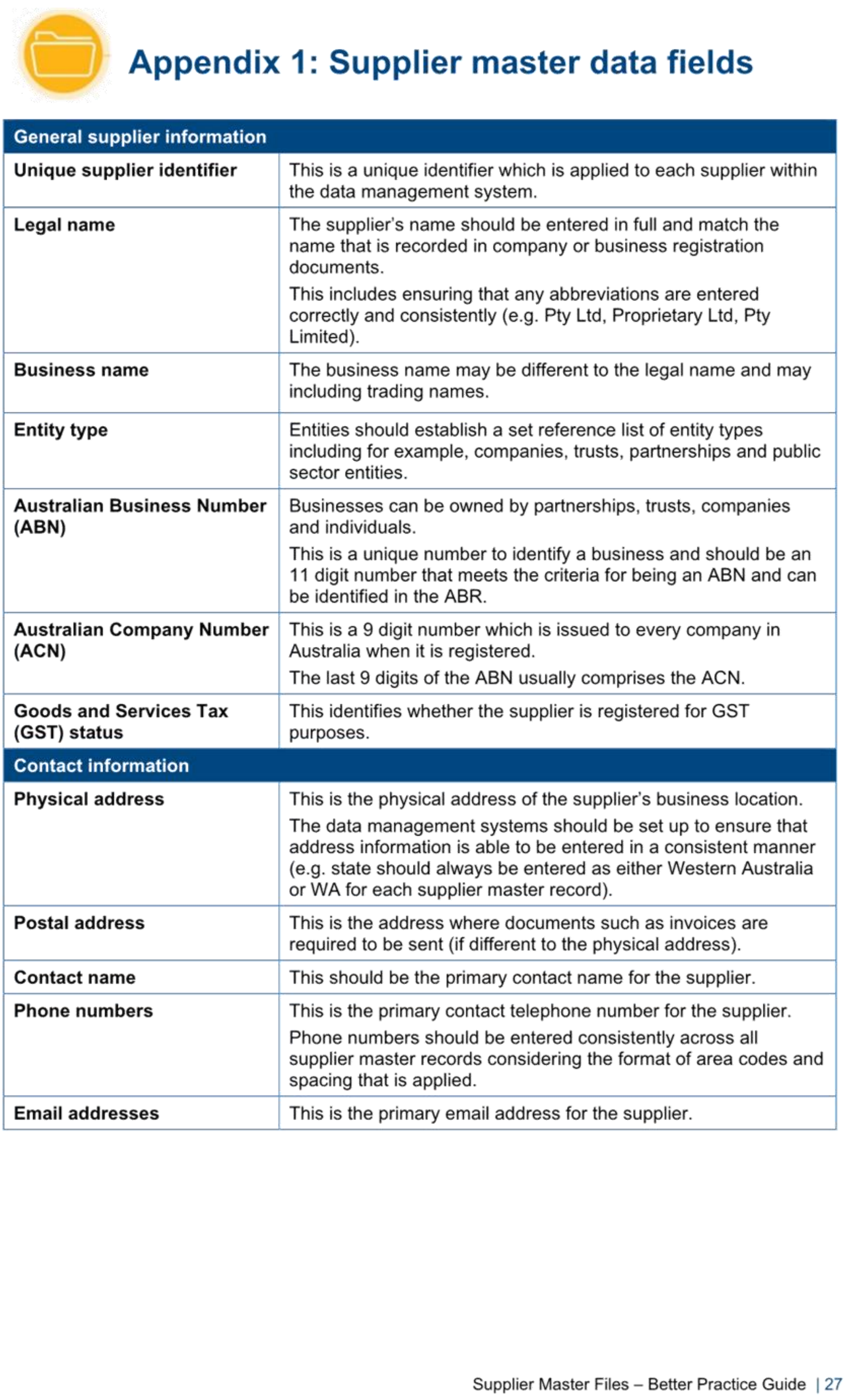
During various audits conducted by our office, we identified that some entities have data management or financial systems with comprehensive audit log capabilities, however these had not been activated. This resulted in key information not being captured about the activities and transactions which were conducted in those systems.

The absence of audit log information can impact an entity's ability to identify and manage risks, ensure accountability, support data integrity, and conduct audits and investigations.

We encourage all entities to explore the audit log capabilities within its various systems and ensure that all audit logs are activated and capturing comprehensive details about the activities being conducted.

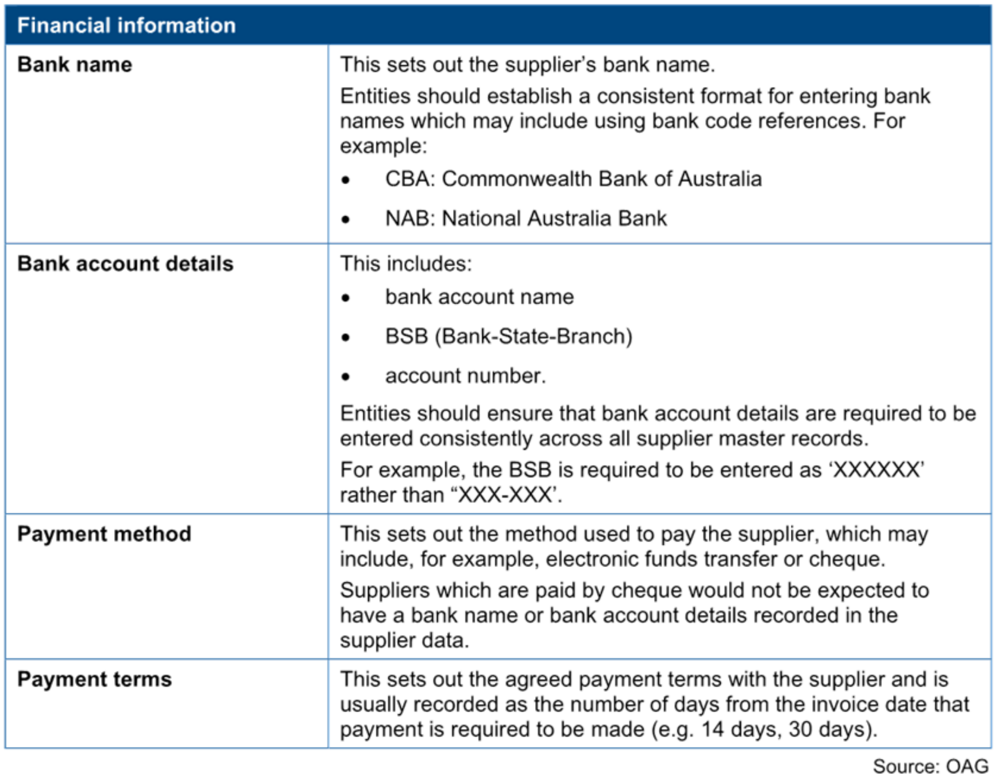
Internal audit programs should include regular audits related to supplier data management. Entities may elect to conduct these audits as a focused examination of supplier data management or otherwise incorporate this into its broader procurement audits.

Internal audits which focus on supplier data management should evaluate the policies, procedures, controls and systems in place to manage supplier master files and its data effectively and focus on assessing the accuracy, completeness and security of supplier master data.



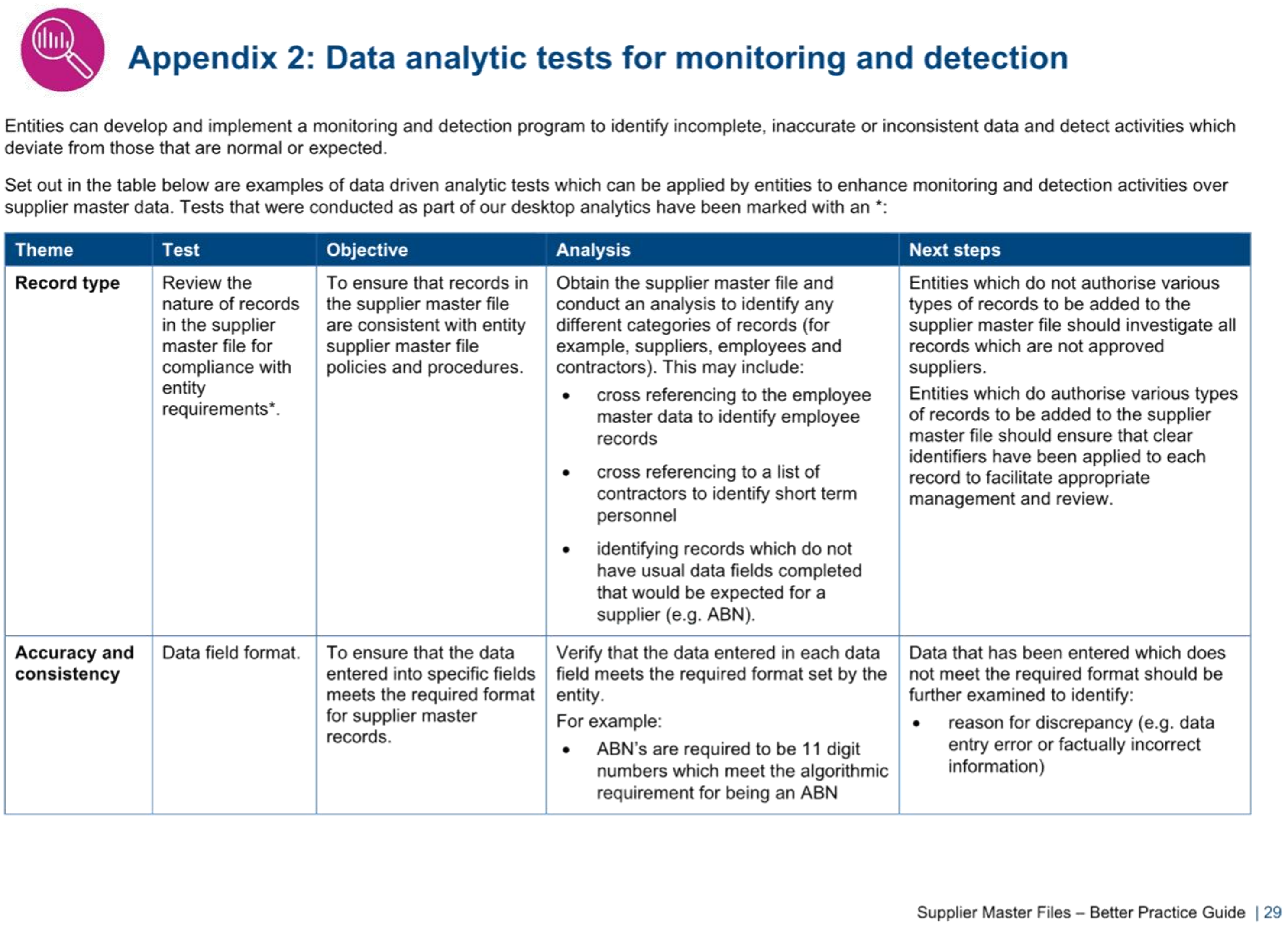
Appendix 1: Supplier master data fields

General supplier information	
Unique supplier identifier	This is a unique identifier which is applied to each supplier within the data management system.
Legal name	The supplier's name should be entered in full and match the name that is recorded in company or business registration documents. This includes ensuring that any abbreviations are entered correctly and consistently (e.g. Pty Ltd, Proprietary Ltd, Pty Limited).
Business name	The business name may be different to the legal name and may including trading names.
Entity type	Entities should establish a set reference list of entity types including for example, companies, trusts, partnerships and public sector entities.
Australian Business Number (ABN)	Businesses can be owned by partnerships, trusts, companies and individuals. This is a unique number to identify a business and should be an 11 digit number that meets the criteria for being an ABN and can be identified in the ABR.
Australian Company Number (ACN)	This is a 9 digit number which is issued to every company in Australia when it is registered. The last 9 digits of the ABN usually comprises the ACN.
Goods and Services Tax (GST) status	This identifies whether the supplier is registered for GST purposes.
Contact information	
Physical address	This is the physical address of the supplier's business location. The data management systems should be set up to ensure that address information is able to be entered in a consistent manner (e.g. state should always be entered as either Western Australia or WA for each supplier master record).
Postal address	This is the address where documents such as invoices are required to be sent (if different to the physical address).
Contact name	This should be the primary contact name for the supplier.
Phone numbers	This is the primary contact telephone number for the supplier. Phone numbers should be entered consistently across all supplier master records considering the format of area codes and spacing that is applied.
Email addresses	This is the primary email address for the supplier.



Financial information	
Bank name	This sets out the supplier's bank name. Entities should establish a consistent format for entering bank names which may include using bank code references. For example: • CBA: Commonwealth Bank of Australia • NAB: National Australia Bank
Bank account details	This includes: • bank account name • BSB (Bank-State-Branch) • account number. Entities should ensure that bank account details are required to be entered consistently across all supplier master records. For example, the BSB is required to be entered as 'XXXXXX' rather than "XXX-XXX'.
Payment method	This sets out the method used to pay the supplier, which may include, for example, electronic funds transfer or cheque. Suppliers which are paid by cheque would not be expected to have a bank name or bank account details recorded in the supplier data.
Payment terms	This sets out the agreed payment terms with the supplier and is usually recorded as the number of days from the invoice date that payment is required to be made (e.g. 14 days, 30 days).

Source: OAG

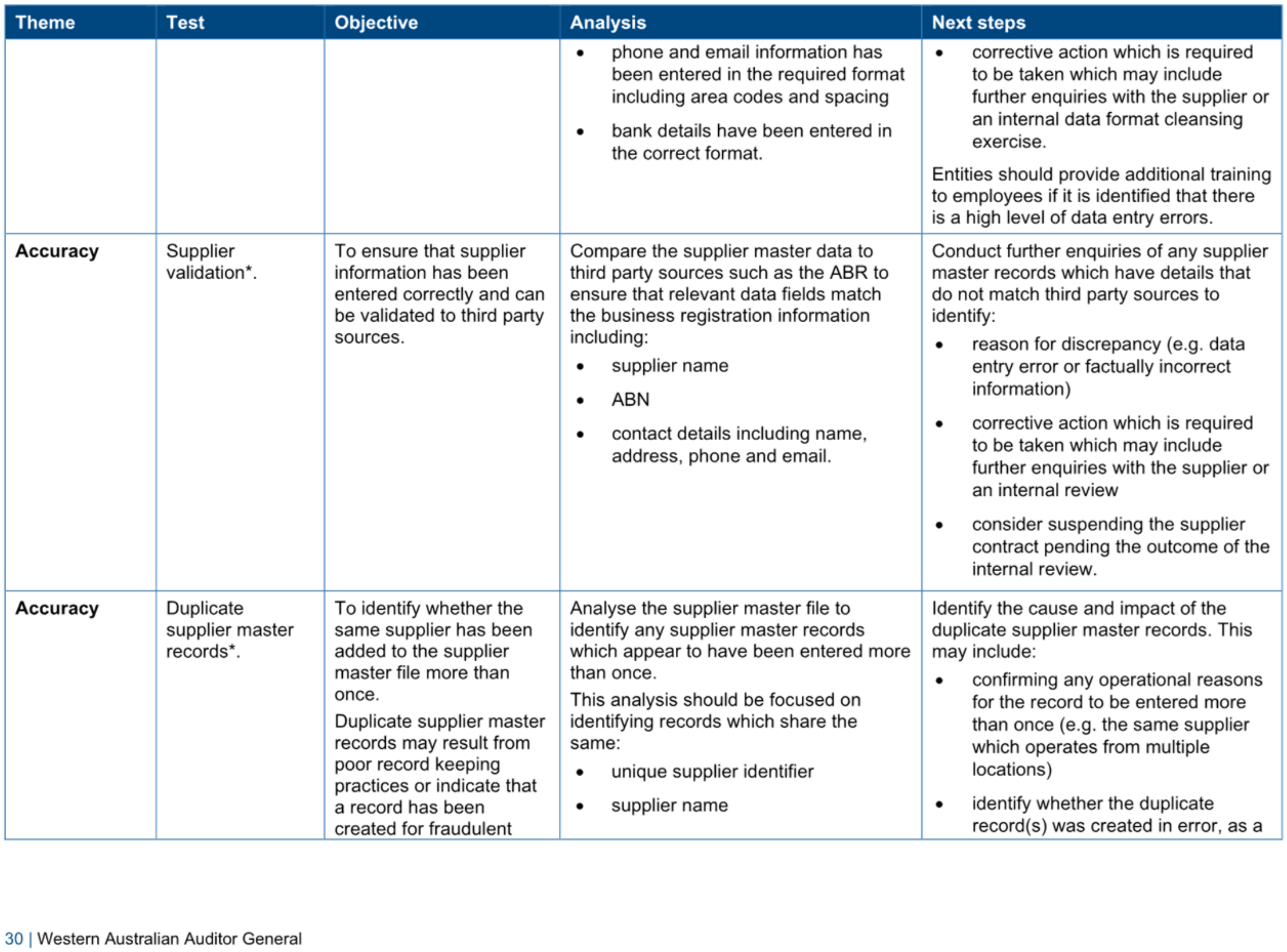


Appendix 2: Data analytic tests for monitoring and detection

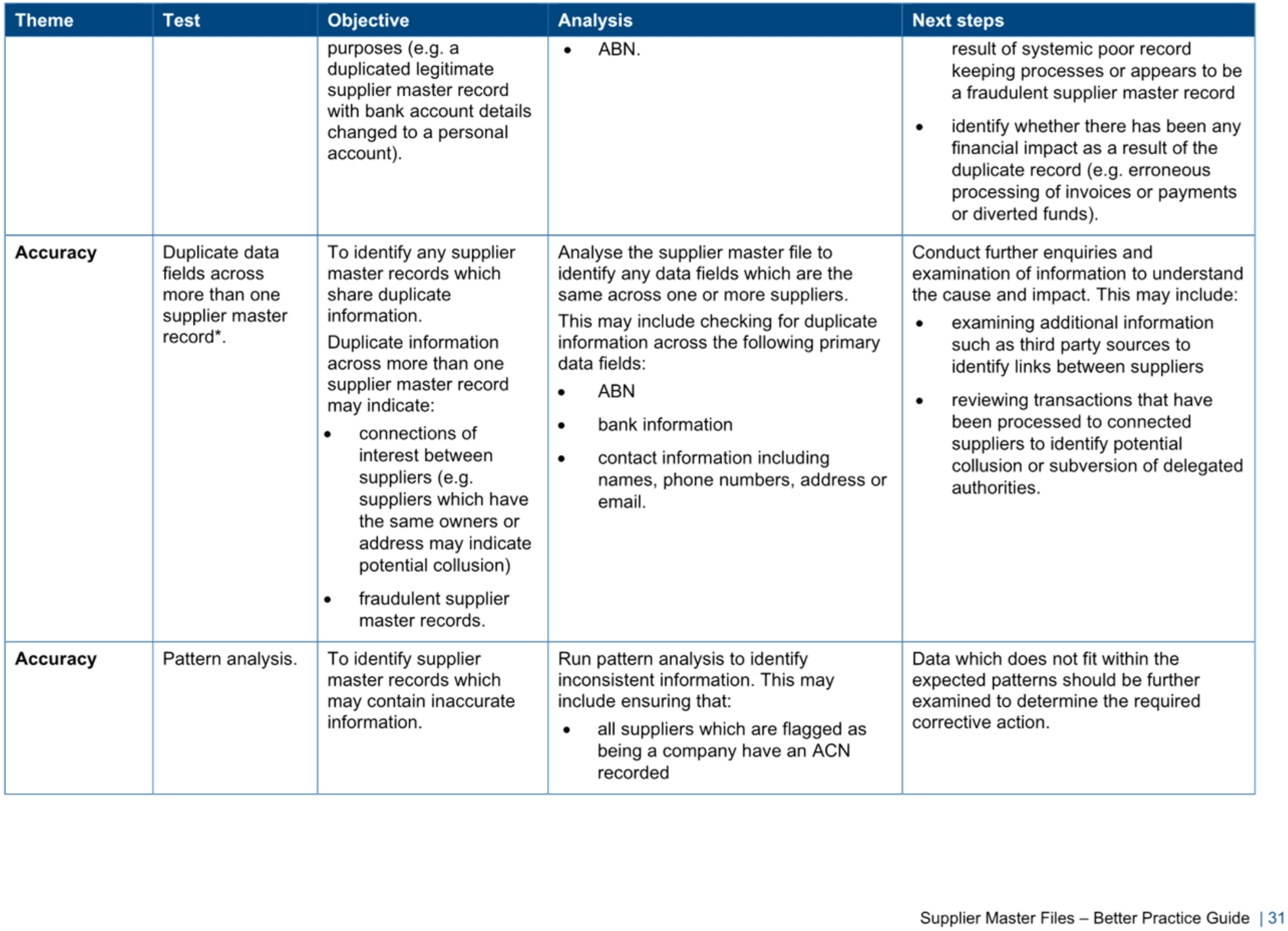
Entities can develop and implement a monitoring and detection program to identify incomplete, inaccurate or inconsistent data and detect activities which deviate from those that are normal or expected.

Set out in the table below are examples of data driven analytic tests which can be applied by entities to enhance monitoring and detection activities over supplier master data. Tests that were conducted as part of our desktop analytics have been marked with an *:

Theme	Test	Objective	Analysis	Next steps
Record type	Review the nature of records in the supplier master file for compliance with entity requirements*.	To ensure that records in the supplier master file are consistent with entity supplier master file policies and procedures.	Obtain the supplier master file and conduct an analysis to identify any different categories of records (for example, suppliers, employees and contractors). This may include: • cross referencing to the employee master data to identify employee records • cross referencing to a list of contractors to identify short term personnel • identifying records which do not have usual data fields completed that would be expected for a supplier (e.g. ABN).	Entities which do not authorise various types of records to be added to the supplier master file should investigate all records which are not approved suppliers. Entities which do authorise various types of records to be added to the supplier master file should ensure that clear identifiers have been applied to each record to facilitate appropriate management and review.
Accuracy and consistency	Data field format.	To ensure that the data entered into specific fields meets the required format for supplier master records.	Verify that the data entered in each data field meets the required format set by the entity. For example: • ABN's are required to be 11 digit numbers which meet the algorithmic requirement for being an ABN	Data that has been entered which does not meet the required format should be further examined to identify: • reason for discrepancy (e.g. data entry error or factually incorrect information)

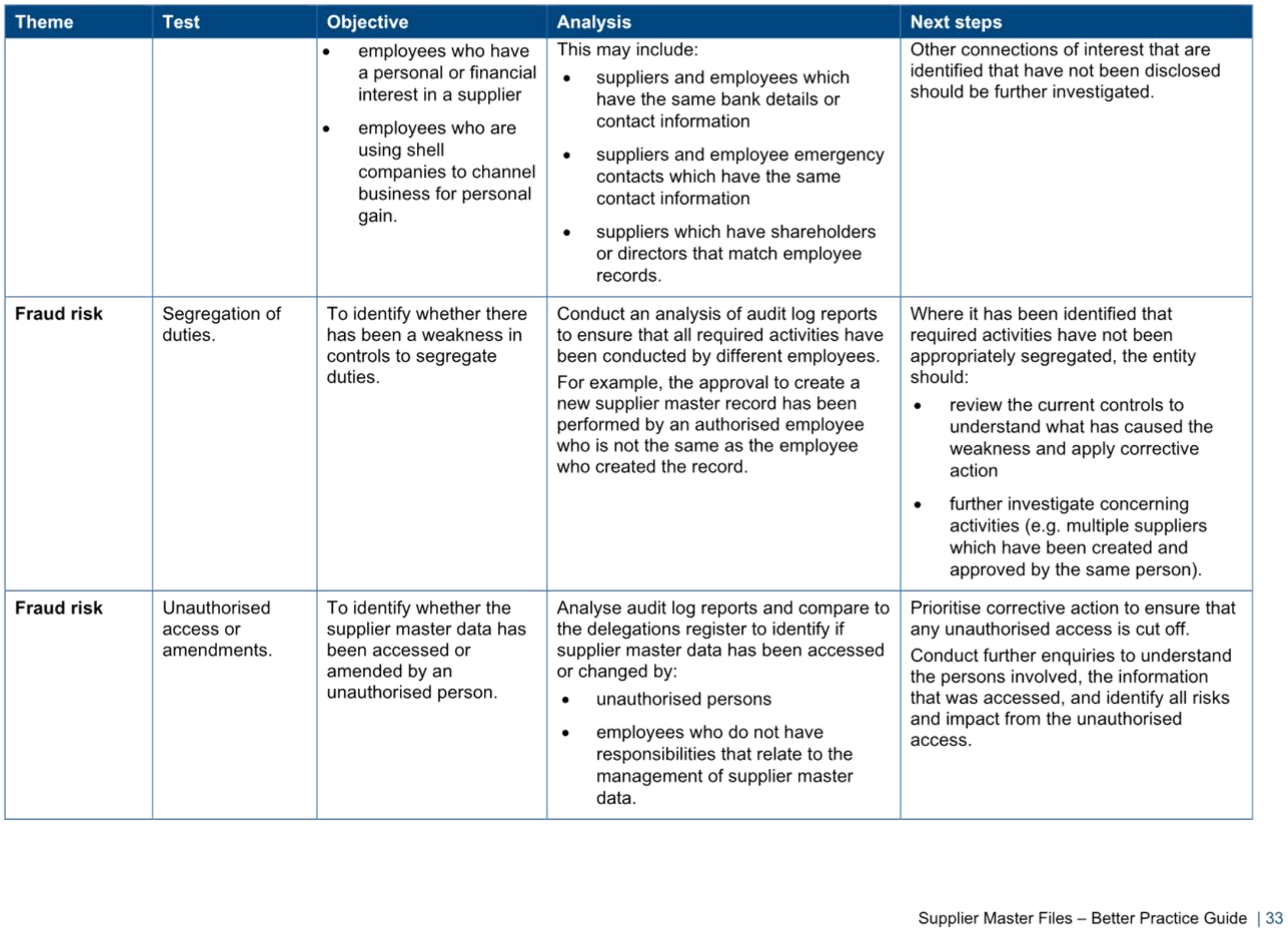


Theme	Test	Objective	Analysis	Next steps
			- phone and email information has been entered in the required format including area codes and spacing - bank details have been entered in the correct format.	- corrective action which is required to be taken which may include further enquiries with the supplier or an internal data format cleansing exercise. Entities should provide additional training to employees if it is identified that there is a high level of data entry errors.
Accuracy	Supplier validation*.	To ensure that supplier information has been entered correctly and can be validated to third party sources.	Compare the supplier master data to third party sources such as the ABR to ensure that relevant data fields match the business registration information including: - supplier name - ABN - contact details including name, address, phone and email.	Conduct further enquiries of any supplier master records which have details that do not match third party sources to identify: - reason for discrepancy (e.g. data entry error or factually incorrect information) - corrective action which is required to be taken which may include further enquiries with the supplier or an internal review - consider suspending the supplier contract pending the outcome of the internal review.
Accuracy	Duplicate supplier master records*.	To identify whether the same supplier has been added to the supplier master file more than once. Duplicate supplier master records may result from poor record keeping practices or indicate that a record has been created for fraudulent	Analyse the supplier master file to identify any supplier master records which appear to have been entered more than once. This analysis should be focused on identifying records which share the same: - unique supplier identifier - supplier name	Identify the cause and impact of the duplicate supplier master records. This may include: - confirming any operational reasons for the record to be entered more than once (e.g. the same supplier which operates from multiple locations) - identify whether the duplicate record(s) was created in error, as a

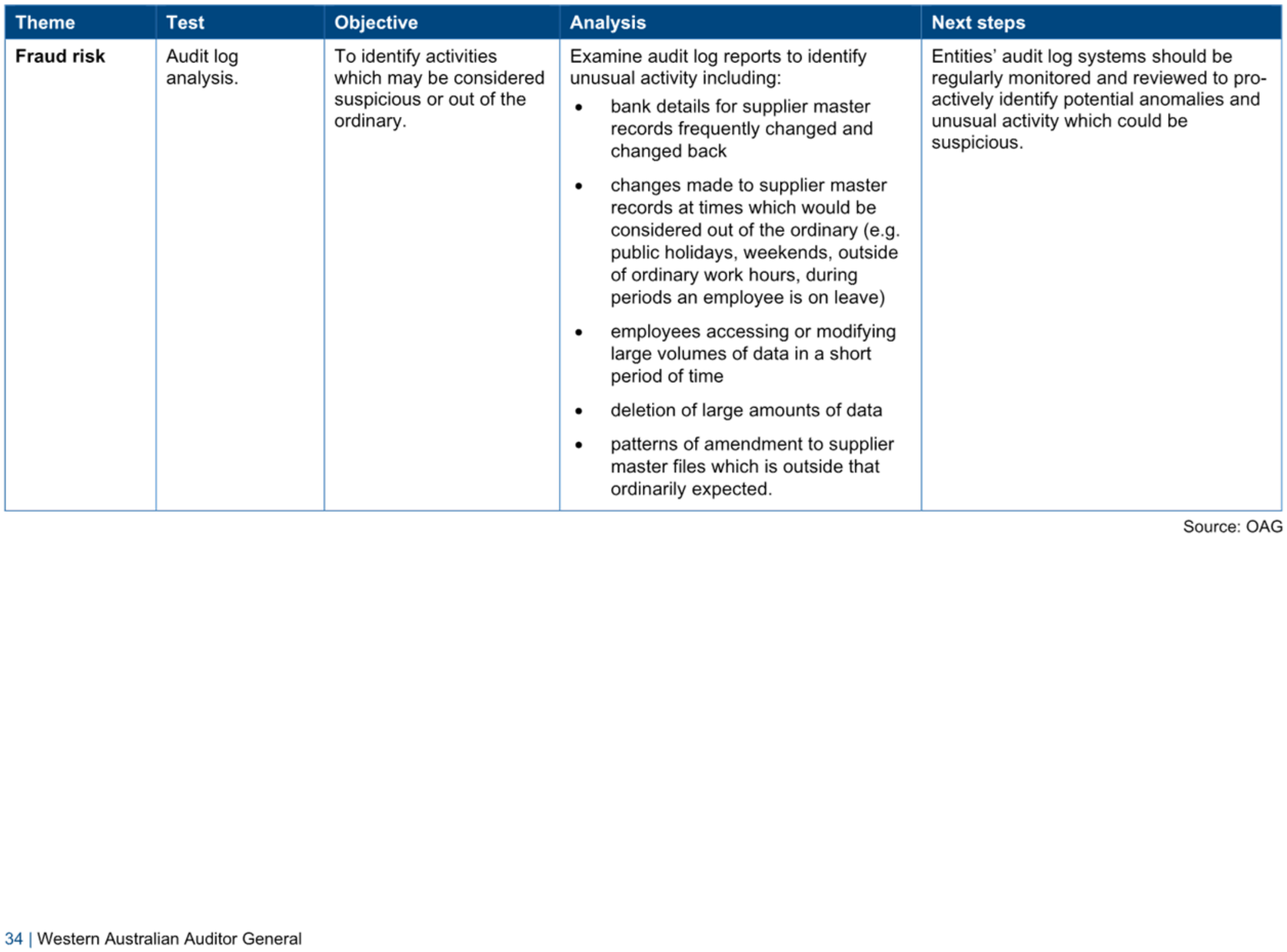


Theme	Test	Objective	Analysis	Next steps
		purposes (e.g. a duplicated legitimate supplier master record with bank account details changed to a personal account).	- ABN.	result of systemic poor record keeping processes or appears to be a fraudulent supplier master record - identify whether there has been any financial impact as a result of the duplicate record (e.g. erroneous processing of invoices or payments or diverted funds).
Accuracy	Duplicate data fields across more than one supplier master record*.	To identify any supplier master records which share duplicate information. Duplicate information across more than one supplier master record may indicate: - connections of interest between suppliers (e.g. suppliers which have the same owners or address may indicate potential collusion) - fraudulent supplier master records.	Analyse the supplier master file to identify any data fields which are the same across one or more suppliers. This may include checking for duplicate information across the following primary data fields: - ABN - bank information - contact information including names, phone numbers, address or email.	Conduct further enquiries and examination of information to understand the cause and impact. This may include: - examining additional information such as third party sources to identify links between suppliers - reviewing transactions that have been processed to connected suppliers to identify potential collusion or subversion of delegated authorities.
Accuracy	Pattern analysis.	To identify supplier master records which may contain inaccurate information.	Run pattern analysis to identify inconsistent information. This may include ensuring that: - all suppliers which are flagged as being a company have an ACN recorded	Data which does not fit within the expected patterns should be further examined to determine the required corrective action.

Theme	Test	Objective	Analysis	Next steps
			• all suppliers from each region have the correct postcode or telephone area code • bank names align with a relevant BSB.	
Accuracy	Dormant suppliers*.	Identify supplier master records which are not actively used in procurement processes.	Conduct an analysis of the supplier master file as compared to supplier payment data to identify any active suppliers which have not been engaged in a payment transaction for a period of time determined by the entity based on its operations (e.g. 18 months).	Conduct further enquiries to determine if the identified suppliers should be marked as inactive in the supplier master file. Further enquiries may include consulting with other business areas including procurement and finance to identify whether there are legitimate reasons the supplier should remain active (e.g. an existing contract). Supplier master records that are confirmed as inactive should be marked accordingly in the supplier master file to ensure that they cannot be used inappropriately.
Completeness	Mandatory data field completeness test.	To identify any supplier master records which have missing information in mandatory data fields. Incomplete supplier data may indicate that due diligence procedures were not complete or the supplier master record may be fictitious.	Analyse the supplier master data to identify any 'blank' or 'null' data fields in mandatory data fields. Refer to Appendix 1 for a list of suggested baseline mandatory data fields.	Missing data should be flagged for further examination and completion. Data entry controls, procedures and approvals should be examined to identify whether these are implemented and working appropriately. Entities should provide additional training to employees if it is identified that there is a high level of data entry errors.
Fraud risk	Employee information recorded in the supplier master file*.	To identify whether there are any connections of interest between suppliers and employees which may include:	Conduct an analysis of the supplier master file as compared to the employee master file to identify any matching data fields which may indicate a connection between employees and suppliers.	The conflict of interest register should be reviewed to identify whether any identified connections have been previously disclosed and are appropriately mitigated.



Theme	Test	Objective	Analysis	Next steps
		- employees who have a personal or financial interest in a supplier - employees who are using shell companies to channel business for personal gain.	This may include: - suppliers and employees which have the same bank details or contact information - suppliers and employee emergency contacts which have the same contact information - suppliers which have shareholders or directors that match employee records.	Other connections of interest that are identified that have not been disclosed should be further investigated.
Fraud risk	Segregation of duties.	To identify whether there has been a weakness in controls to segregate duties.	Conduct an analysis of audit log reports to ensure that all required activities have been conducted by different employees. For example, the approval to create a new supplier master record has been performed by an authorised employee who is not the same as the employee who created the record.	Where it has been identified that required activities have not been appropriately segregated, the entity should: - review the current controls to understand what has caused the weakness and apply corrective action - further investigate concerning activities (e.g. multiple suppliers which have been created and approved by the same person).
Fraud risk	Unauthorised access or amendments.	To identify whether the supplier master data has been accessed or amended by an unauthorised person.	Analyse audit log reports and compare to the delegations register to identify if supplier master data has been accessed or changed by: - unauthorised persons - employees who do not have responsibilities that relate to the management of supplier master data.	Prioritise corrective action to ensure that any unauthorised access is cut off. Conduct further enquiries to understand the persons involved, the information that was accessed, and identify all risks and impact from the unauthorised access.



Theme	Test	Objective	Analysis	Next steps
Fraud risk	Audit log analysis.	To identify activities which may be considered suspicious or out of the ordinary.	Examine audit log reports to identify unusual activity including: • bank details for supplier master records frequently changed and changed back • changes made to supplier master records at times which would be considered out of the ordinary (e.g. public holidays, weekends, outside of ordinary work hours, during periods an employee is on leave) • employees accessing or modifying large volumes of data in a short period of time • deletion of large amounts of data • patterns of amendment to supplier master files which is outside that ordinarily expected.	Entities' audit log systems should be regularly monitored and reviewed to pro-actively identify potential anomalies and unusual activity which could be suspicious.

Source: OAG

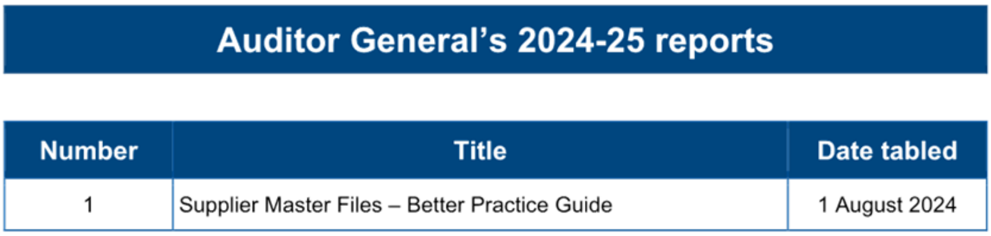
Appendix 3: Additional resources

The additional resources listed may be useful to entities in implementing or improving their current supplier data management practices.

Entity	Description	Link
Office of the Auditor General Western Australia	Report 20 – Fraud Risk Management – Better Practice Guide June 2022	https://audit.wa.gov.au/reports-and-publications/reports/fraud-risk-management-better-practice-guide/
Office of the Auditor General Western Australia	Report 12 – Digital Identity and Access Management – Better Practice Guide March 2024	https://audit.wa.gov.au/reports-and-publications/reports/digital-identity-and-access-management-better-practice-guide/
Office of the Auditor General Western Australia	Report 25 – Staff Exit Controls at Large Local Government Entities	https://audit.wa.gov.au/reports-and-publications/reports/staff-exit-controls-at-large-local-government-entities/
Office of the Auditor General Western Australia	Report 3 – Staff Exit Controls August 2021	https://audit.wa.gov.au/reports-and-publications/reports/staff-exit-controls/
Office of the Auditor General Western Australia	Report 16 – Management of Supplier Master Files March 2019	https://audit.wa.gov.au/reports-and-publications/reports/management-of-supplier-master-files/appendix-1/
Department of Treasury	Treasurer's Instructions including: • TI 4 Risk Management & Internal Control | Requirement 2: Risk Management • TI 5 Expenditure and Payments | Requirement 1: Authorisation of Payments (segregation of duties) • TI 8 Financial Accounting and Reporting | Requirement 1: Requirements of Accounting Systems • TI 10 Internal Audit | Requirement 1: Internal Audit	https://www.wa.gov.au/government/publications/financial-administration-bookcase
Department of Finance	Western Australian Procurement Rules	https://www.wa.gov.au/government/publications/general-procurement-direction-202401-western-australian-procurement-rules
Department of Finance	Preventing procurement fraud	https://www.wa.gov.au/service/government-financial-management/procurement/preventing-procurement-fraud
Public Sector Commission	Integrity Framework resources	https://www.wa.gov.au/organisation/public-sector-commission/integrity-framework-resources
Public Sector Commission	Developing Detection Systems	https://www.wa.gov.au/government/multi-step-guides/developing-detection-systems

Entity	Description	Link
Public Sector Commission	Conflicts of Interest Guide	https://www.wa.gov.au/government/multi-step-guides/conflicts-of-interest-guide
Public Sector Commission	A guide to public interest disclosures in WA public authorities	https://www.wa.gov.au/organisation/public-sector-commission/guide-public-interest-disclosures-wa-public-authorities
Public Sector Commission	Strengthening integrity in financial management	https://www.wa.gov.au/organisation/public-sector-commission/strengthening-integrity-financial-management
Public Sector Commission	Integrity in financial management: Self assessment checklist	https://www.wa.gov.au/government/publications/integrity-financial-management-self-assessment-checklist
Public Sector Commission and Corruption and Crime Commission	Notifying misconduct – A guide for Principal Officers of notifying authorities August 2018	https://www.ccc.wa.gov.au/media/resources
Australian Government: **Australian Business Register**	Format of the ABN	https://abr.business.gov.au/Help/AbnFormat
Australian Government: **Australian Business Register**	Type of entity: Entity mapping file	https://www.abr.gov.au/government-agencies/accessing-abr-data/abr-data-dictionary/entity-mapping-file
Office of Digital Government	2024 WA Government Cyber Security Policy	https://www.wa.gov.au/government/publications/2024-wa-government-cyber-security-policy

Source: OAG



Auditor General's 2024-25 reports

Number	Title	Date tabled
1	Supplier Master Files – Better Practice Guide	1 August 2024

Office of the Auditor General for 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 REVIEW OF FRAUD AND CORRUPTION PREVENTION POLICY

Attachments: 1. Updated Fraud and Corruption Policy - Draft ⇩

RECOMMENDATION:

That the Audit and Risk Committee recommends to Council that it:

1. **RECEIVES the review of the Fraud and Corruption Prevention Policy; and**

2. **SUPPORTS the presentation of the updated Fraud and Corruption Prevention Policy, as detailed in Attachment 1, to Council for approval to advertise.**

<u>COMMITTEE DECISION ITEM 5.2</u>

<u>Moved:</u> Mayor Xamon, <u>Seconded:</u> Mr Manifis

That the recommendation be adopted.

<u>CARRIED (6-0)</u>

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

CITY OF VINCENT

FRAUD AND CORRUPTION PREVENTION POLICY

Legislation / local law requirements	- *Public Interest Disclosure Act 2003 (PID Act)* - *Corruption, Crime and Misconduct Act 2003* - *Local Government (Financial Management) Regulations 1996* - *Local Government (Audit) Regulations 1996*
Relevant delegations	17.1.1 - Appointment of Public Interest Disclosure Officer
Related policies, procedures and supporting documentation	- Integrity Framework - Governance Framework - Risk Management Framework - Fraud and Corruption Risk Register - Code of Conduct - Public Interest Disclosure Guidelines - Australian Standard AS 8001:2021 – Fraud and Corruption Control - OAG Better Practice Guide

PRELIMINARY

INTRODUCTION

Fraud and corruption pose significant risks to the integrity and effectiveness of any organisation. These unethical practices can lead to financial losses, damage to reputation, and a decrease in public trust. The City recognises the importance of maintaining a robust framework to prevent, detect, and respond to fraud and corruption. This policy outlines the City's commitment to upholding the highest standards of integrity and ethical behaviour, ensuring that all employees and stakeholders act in accordance with established guidelines and procedures. By implementing comprehensive measures for prevention, reporting, and investigation, the City aims to foster a culture of transparency and accountability.

PURPOSE

The purpose of this policy is to:

- Demonstrate the City's zero tolerance for fraud and corruption in all operations;
- Support the City's Integrity Framework by providing a high-level approach to fraud and corruption prevention, detection, and response;
- Promote ethical behaviour, accountability, and public trust by safeguarding the City's resources and reputation.

OBJECTIVE

The objective of this policy is to:

1. Prevent fraud and corruption by embedding a culture of integrity and ethical behaviour;
2. Detect fraud and corruption through effective risk management and reporting mechanisms;
3. Respond promptly and effectively to suspected or actual incidents of fraud or corruption;
4. Ensure alignment with the City's Integrity Framework, which provides detailed roles, responsibilities, and operational guidance.

FRAUD AND CORRUPTION PREVENTION POLICY

SCOPE

This policy applies to:

- All Council Members, employees, contractors, and volunteers;
- All activities, decisions, and services undertaken on behalf of the City.

DEFINITIONS

Fraud: Dishonest activity causing actual or potential gain or loss to any person or organisation, including theft of money or property by persons internal or external to the organisation. Fraud may also involve deception, misrepresentation, or the misuse of position or authority to achieve an unlawful or unfair benefit (Australian Standard AS 8001:2021).

Corruption: Dishonest or unethical activity by a person in a position of trust (e.g., director, employee, contractor) that breaches their duty to act in the best interests of the organisation. This can include abuse of position, conflicts of interest, or collusion to secure a personal or improper advantage (Australian Standard AS 8001:2021).

Fraud and Corruption Control System (FCCS): Framework for controlling the risk of fraud and corruption against or by and organisation.

Integrity Framework: A guiding document that integrates the City's principles, policies, and practices to promote ethical behaviour, accountability, and compliance. It links internal controls, audits, governance systems, and continuous improvement processes to prevent, detect, and respond to misconduct, creating a shared understanding of integrity across the organisation.

Fraud and Corruption Risk Register: A comprehensive tool that identifies and analyses the City's vulnerabilities to fraud and corruption, prioritising high-risk areas, control effectiveness and risk management actions.

Risk Management Framework: Suite of interconnected documents that guide how the City identifies, analyses, treats, and reports on risks

FRAUD AND CORRUPTION PREVENTION POLICY

CITY OF VINCENT

POLICY PROVISIONS

POLICY

1. Commitment to Integrity

The City is committed to:

- Maintaining robust systems and controls to prevent and detect fraud and corruption;
- Ensuring all employees and stakeholders act in accordance with the Integrity Framework;
- Investigating all allegations of fraud and corruption promptly and confidentially;
- Meeting statutory obligations to report serious misconduct to external oversight bodies where necessary.

2. Fraud and Corruption Prevention

Fraud and corruption prevention will be achieved by:

- Managing risks through the Fraud and Corruption Risk Register and Corporate Risk Register;
- Implementing strong internal controls, including segregation of duties and validation procedures;
- Conducting fraud awareness training to ensure staff and Council Members understand their obligations;
- Encouraging ethical behaviour as outlined in the City's Code of Conduct and Integrity Framework.

3. Reporting and Investigation

- The City will provide confidential and accessible mechanisms for reporting suspected fraud or corruption, as detailed in the Integrity Framework.
- Investigations will be conducted fairly, transparently, and in accordance with legislative requirements.
- The City will take appropriate corrective action, including referral to external agencies such as the Corruption and Crime Commission (CCC) or WA Police, where required.

4. Oversight and Review

- Oversight of fraud and corruption prevention activities will be conducted in alignment with the City's Integrity Framework.
- This policy will be reviewed biennially, or earlier, if necessary, to ensure its continued effectiveness and relevance.

FRAUD AND CORRUPTION PREVENTION POLICY

CITY OF VINCENT

OFFICE USE ONLY	
Responsible Officer	Please use title only
Initial Council Adoption	DD/MM/YYYY
Previous Title	Applicable if the policy has been renamed
Reviewed / Amended	DD/MM/YYYY
Next Review Date	MM/YYYY

5.3 LOCAL GOVERNMENT STATUTORY COMPLIANCE AUDIT RETURN 2024

Attachments: 1. Compliance Audit Return 2025 ⇩

RECOMMENDATION:

That the Audit Committee RECOMMENDS that Council adopts the Local Government Statutory Compliance Audit Return for the period 1 January 2024 to 31 December 2024.

COMMITTEE DECISION ITEM 5.3

Moved: Mr Manifis, Seconded: Cr Hallett

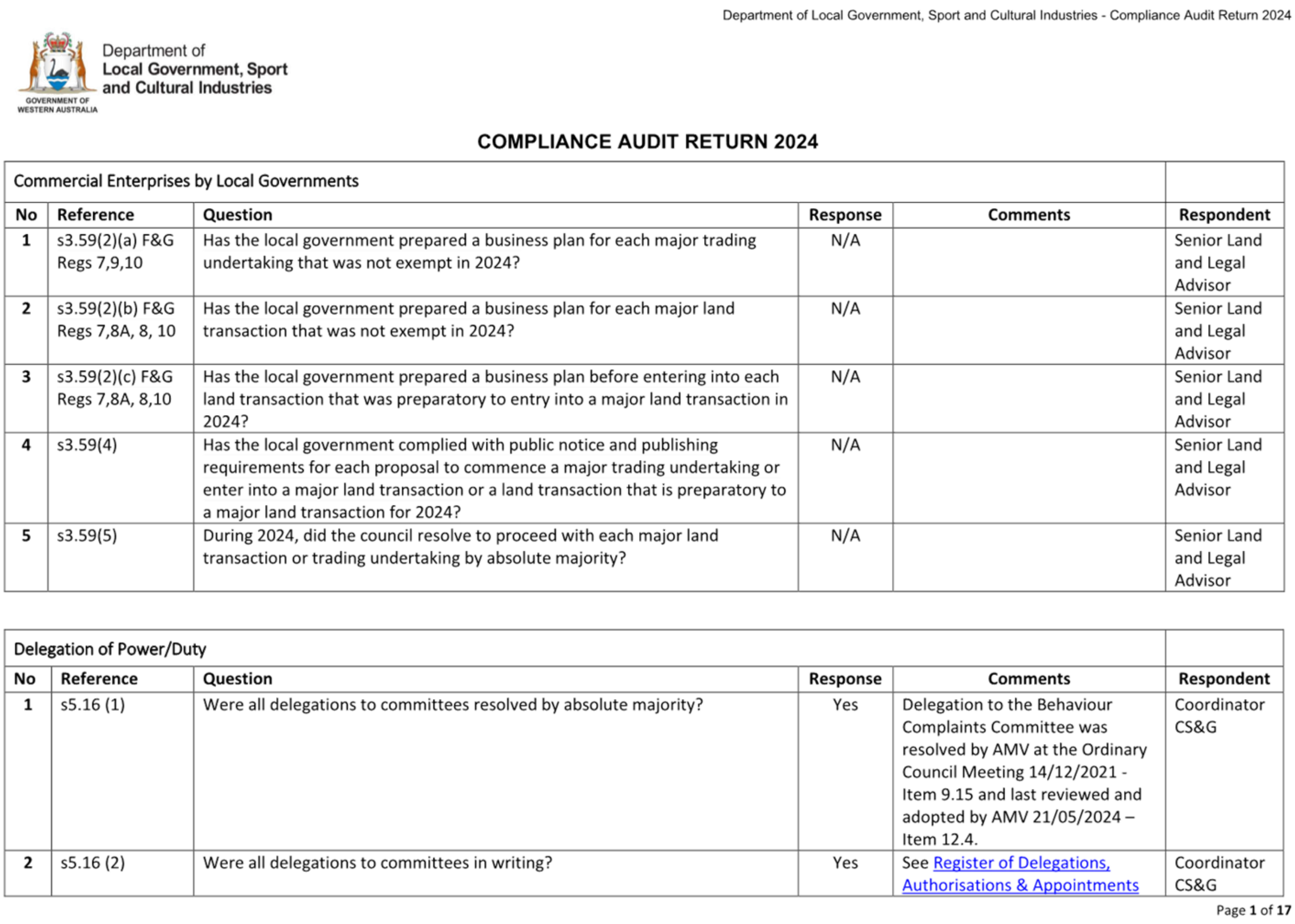
That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)



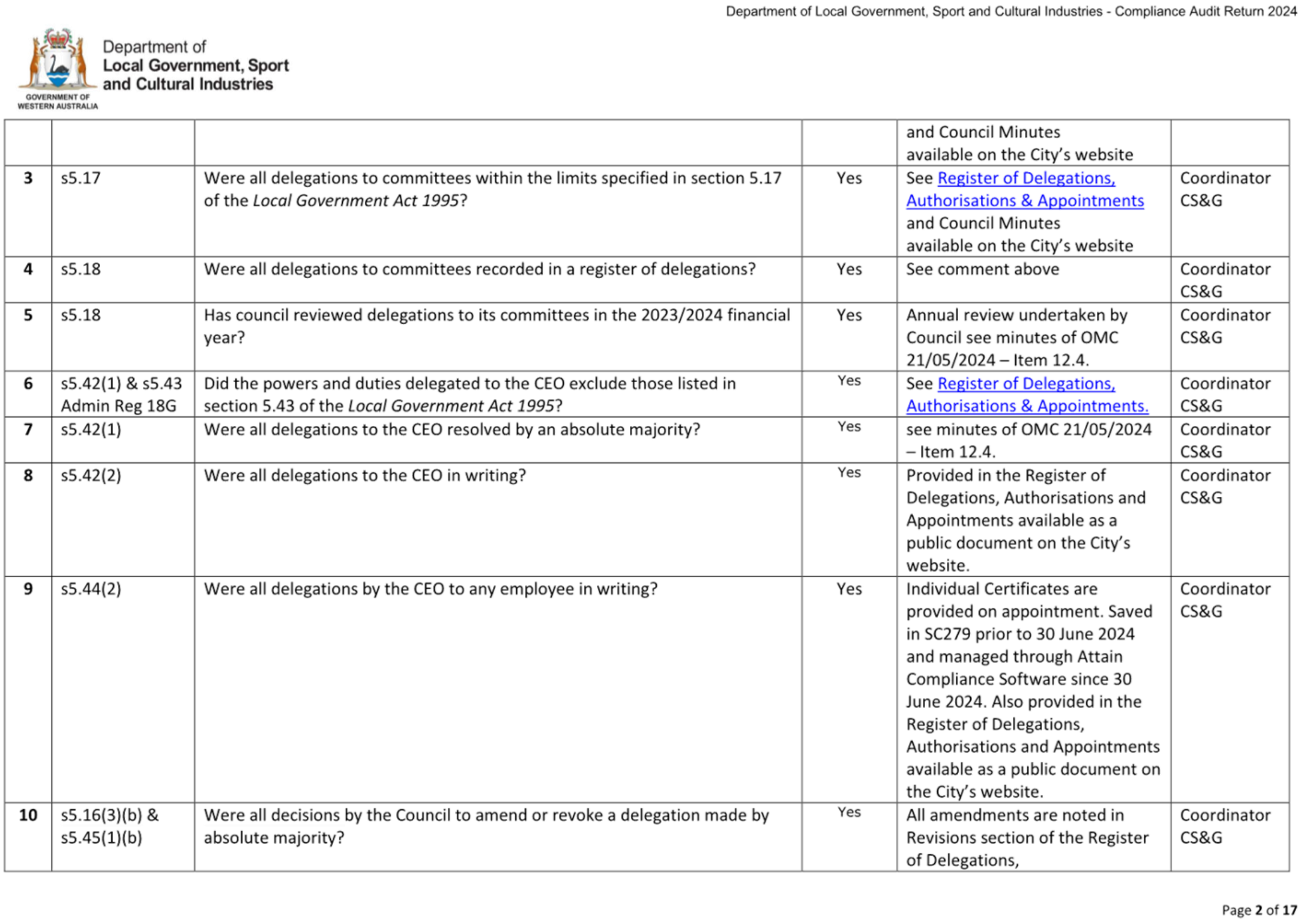
GOVERNMENT OF WESTERN AUSTRALIA

Department of
Local Government, Sport
and Cultural Industries

COMPLIANCE AUDIT RETURN 2024

Commercial Enterprises by Local Governments					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s3.59(2)(a) F&G Regs 7,9,10	Has the local government prepared a business plan for each major trading undertaking that was not exempt in 2024?	N/A		Senior Land and Legal Advisor
2	s3.59(2)(b) F&G Regs 7,8A, 8, 10	Has the local government prepared a business plan for each major land transaction that was not exempt in 2024?	N/A		Senior Land and Legal Advisor
3	s3.59(2)(c) F&G Regs 7,8A, 8,10	Has the local government prepared a business plan before entering into each land transaction that was preparatory to entry into a major land transaction in 2024?	N/A		Senior Land and Legal Advisor
4	s3.59(4)	Has the local government complied with public notice and publishing requirements for each proposal to commence a major trading undertaking or enter into a major land transaction or a land transaction that is preparatory to a major land transaction for 2024?	N/A		Senior Land and Legal Advisor
5	s3.59(5)	During 2024, did the council resolve to proceed with each major land transaction or trading undertaking by absolute majority?	N/A		Senior Land and Legal Advisor

Delegation of Power/Duty					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s5.16 (1)	Were all delegations to committees resolved by absolute majority?	Yes	Delegation to the Behaviour Complaints Committee was resolved by AMV at the Ordinary Council Meeting 14/12/2021 - Item 9.15 and last reviewed and adopted by AMV 21/05/2024 – Item 12.4.	Coordinator CS&G
2	s5.16 (2)	Were all delegations to committees in writing?	Yes	See Register of Delegations, Authorisations & Appointments	Coordinator CS&G



Department of
Local Government, Sport and Cultural Industries
GOVERNMENT OF WESTERN AUSTRALIA

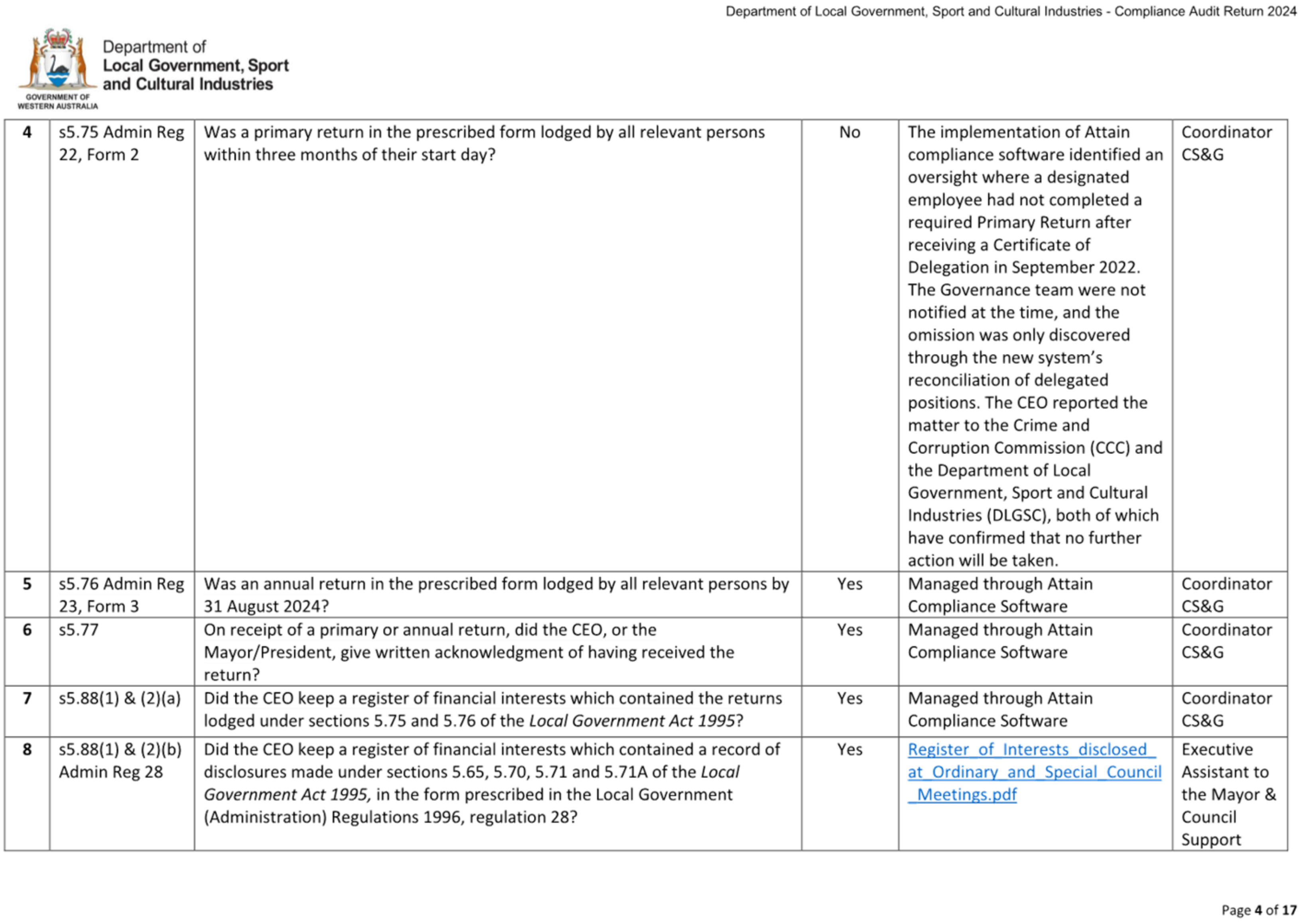
				and Council Minutes available on the City's website	
3	s5.17	Were all delegations to committees within the limits specified in section 5.17 of the *Local Government Act 1995*?	Yes	See Register of Delegations, Authorisations & Appointments and Council Minutes available on the City's website	Coordinator CS&G
4	s5.18	Were all delegations to committees recorded in a register of delegations?	Yes	See comment above	Coordinator CS&G
5	s5.18	Has council reviewed delegations to its committees in the 2023/2024 financial year?	Yes	Annual review undertaken by Council see minutes of OMC 21/05/2024 – Item 12.4.	Coordinator CS&G
6	s5.42(1) & s5.43 Admin Reg 18G	Did the powers and duties delegated to the CEO exclude those listed in section 5.43 of the *Local Government Act 1995*?	Yes	See Register of Delegations, Authorisations & Appointments.	Coordinator CS&G
7	s5.42(1)	Were all delegations to the CEO resolved by an absolute majority?	Yes	see minutes of OMC 21/05/2024 – Item 12.4.	Coordinator CS&G
8	s5.42(2)	Were all delegations to the CEO in writing?	Yes	Provided in the Register of Delegations, Authorisations and Appointments available as a public document on the City's website.	Coordinator CS&G
9	s5.44(2)	Were all delegations by the CEO to any employee in writing?	Yes	Individual Certificates are provided on appointment. Saved in SC279 prior to 30 June 2024 and managed through Attain Compliance Software since 30 June 2024. Also provided in the Register of Delegations, Authorisations and Appointments available as a public document on the City's website.	Coordinator CS&G
10	s5.16(3)(b) & s5.45(1)(b)	Were all decisions by the Council to amend or revoke a delegation made by absolute majority?	Yes	All amendments are noted in Revisions section of the Register of Delegations,	Coordinator CS&G

Department of
Local Government, Sport
and Cultural Industries

GOVERNMENT OF
WESTERN AUSTRALIA

				Authorisations and Appointments	
11	s5.46(1)	Has the CEO kept a register of all delegations made under Division 4 of the Act to the CEO and to employees?	Yes	See Register of Delegations, Authorisations & Appointments available as a public document on the City's website.	Coordinator CS&G
12	s5.46(2)	Were all delegations made under Division 4 of the Act reviewed by the delegator at least once during the 2023/2024 financial year?	Yes	Annual review undertaken by administration 21/03/2024 & by Council at OMC 21/05/2024 Item 12.4.	Coordinator CS&G
13	s5.46(3) Admin Reg 19	Did all persons exercising a delegated power or duty under the Act keep, on all occasions, a written record in accordance with *Local Government (Administration) Regulations 1996,* regulation 19?	Yes	Saved to the City's central record keeping system (Content Manager).	Coordinator CS&G

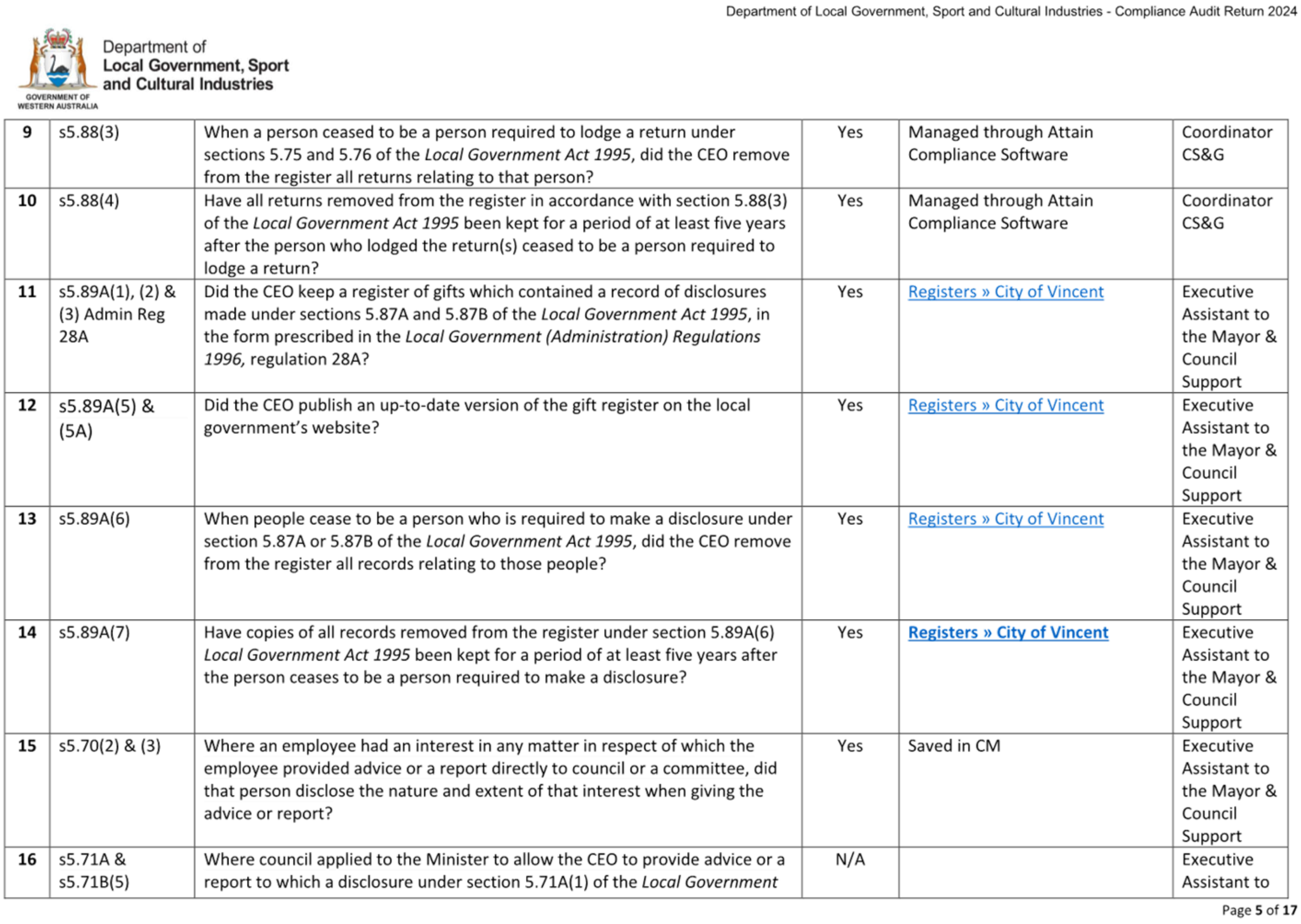
Disclosure of Interest					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s5.67	Where a council member disclosed an interest in a matter and did not have participation approval under sections 5.68 or 5.69 of the *Local Government Act 1995,* did the council member ensure that they did not remain present to participate in discussion or decision making relating to the matter?	Yes	The council member leaving was recorded in the minutes prior to the relevant item.	Executive Assistant to the Mayor & Council Support
2	s5.68(2) & s5.69(5) Admin Reg 21A	Were all decisions regarding participation approval, including the extent of participation allowed and, where relevant, the information required by the *Local Government (Administration) Regulations 1996* regulation 21A, recorded in the minutes of the relevant council or committee meeting?	N/A		Executive Assistant to the Mayor & Council Support
3	s5.73	Were disclosures under sections 5.65, 5.70 or 5.71A(3) of the *Local Government Act 1995* recorded in the minutes of the meeting at which the disclosures were made?	Yes	No employee declarations, all others recorded in the minutes	Executive Assistant to the Mayor & Council Support



Department of
Local Government, Sport
and Cultural Industries

GOVERNMENT OF
WESTERN AUSTRALIA

4	s5.75 Admin Reg 22, Form 2	Was a primary return in the prescribed form lodged by all relevant persons within three months of their start day?	No	The implementation of Attain compliance software identified an oversight where a designated employee had not completed a required Primary Return after receiving a Certificate of Delegation in September 2022. The Governance team were not notified at the time, and the omission was only discovered through the new system's reconciliation of delegated positions. The CEO reported the matter to the Crime and Corruption Commission (CCC) and the Department of Local Government, Sport and Cultural Industries (DLGSC), both of which have confirmed that no further action will be taken.	Coordinator CS&G
5	s5.76 Admin Reg 23, Form 3	Was an annual return in the prescribed form lodged by all relevant persons by 31 August 2024?	Yes	Managed through Attain Compliance Software	Coordinator CS&G
6	s5.77	On receipt of a primary or annual return, did the CEO, or the Mayor/President, give written acknowledgment of having received the return?	Yes	Managed through Attain Compliance Software	Coordinator CS&G
7	s5.88(1) & (2)(a)	Did the CEO keep a register of financial interests which contained the returns lodged under sections 5.75 and 5.76 of the *Local Government Act 1995*?	Yes	Managed through Attain Compliance Software	Coordinator CS&G
8	s5.88(1) & (2)(b) Admin Reg 28	Did the CEO keep a register of financial interests which contained a record of disclosures made under sections 5.65, 5.70, 5.71 and 5.71A of the *Local Government Act 1995,* in the form prescribed in the Local Government (Administration) Regulations 1996, regulation 28?	Yes	Register_of_Interests_disclosed_at_Ordinary_and_Special_Council_Meetings.pdf	Executive Assistant to the Mayor & Council Support



9	s5.88(3)	When a person ceased to be a person required to lodge a return under sections 5.75 and 5.76 of the *Local Government Act 1995*, did the CEO remove from the register all returns relating to that person?	Yes	Managed through Attain Compliance Software	Coordinator CS&G
10	s5.88(4)	Have all returns removed from the register in accordance with section 5.88(3) of the *Local Government Act 1995* been kept for a period of at least five years after the person who lodged the return(s) ceased to be a person required to lodge a return?	Yes	Managed through Attain Compliance Software	Coordinator CS&G
11	s5.89A(1), (2) & (3) Admin Reg 28A	Did the CEO keep a register of gifts which contained a record of disclosures made under sections 5.87A and 5.87B of the *Local Government Act 1995*, in the form prescribed in the *Local Government (Administration) Regulations 1996*, regulation 28A?	Yes	Registers » City of Vincent	Executive Assistant to the Mayor & Council Support
12	s5.89A(5) & (5A)	Did the CEO publish an up-to-date version of the gift register on the local government's website?	Yes	Registers » City of Vincent	Executive Assistant to the Mayor & Council Support
13	s5.89A(6)	When people cease to be a person who is required to make a disclosure under section 5.87A or 5.87B of the *Local Government Act 1995*, did the CEO remove from the register all records relating to those people?	Yes	Registers » City of Vincent	Executive Assistant to the Mayor & Council Support
14	s5.89A(7)	Have copies of all records removed from the register under section 5.89A(6) *Local Government Act 1995* been kept for a period of at least five years after the person ceases to be a person required to make a disclosure?	Yes	**Registers » City of Vincent**	Executive Assistant to the Mayor & Council Support
15	s5.70(2) & (3)	Where an employee had an interest in any matter in respect of which the employee provided advice or a report directly to council or a committee, did that person disclose the nature and extent of that interest when giving the advice or report?	Yes	Saved in CM	Executive Assistant to the Mayor & Council Support
16	s5.71A & s5.71B(5)	Where council applied to the Minister to allow the CEO to provide advice or a report to which a disclosure under section 5.71A(1) of the *Local Government*	N/A		Executive Assistant to

		Act 1995 relates, did the application include details of the nature of the interest disclosed and any other information required by the Minister for the purposes of the application?			the Mayor & Council Support
17	s5.71B(6) & s5.71B(7)	Was any decision made by the Minister under section 5.71B(6) of the *Local Government Act 1995,* recorded in the minutes of the council meeting at which the decision was considered?	N/A		Executive Assistant to the Mayor & Council Support
18	s5.104(1)	Did the local government prepare and adopt, by absolute majority, a code of conduct to be observed by council members, committee members and candidates that incorporates the model code of conduct?	Yes	At the 23 March 2021 Ordinary Meeting of Council, a new Code of Conduct to be observed by Council Members, Committee Members and Candidates that incorporates the Model Code was adopted.	Coordinator CS&G
19	s5.104(3) & (4)	Did the local government adopt additional requirements in addition to the model code of conduct? If yes, does it comply with section 5.104(3) and (4) of the *Local Government Act 1995*?	Yes	Administration proposed some minor amendments to the Model Code Division 3 (Behaviours) to incorporate behaviours referred to in the 2017 Code. All amendments comply with section 5.104(3) and (4)	Coordinator CS&G
20	s5.104(7)	Has the CEO published an up-to-date version of the code of conduct for council members, committee members and candidates on the local government's website?	Yes	Located under 'Code of conduct and CEO standards' Available on the City's website Code of Conduct	Coordinator CS&G

21	s5.51A(1) & (3)	Has the CEO prepared and implemented a code of conduct to be observed by employee of the local government? If yes, has the CEO published an up-to-date version of the code of conduct for employees on the local government's website?	Yes	The Code of Conduct for City of Vincent Employees and Contractors has been developed and implemented by the CEO. Available on the City's website	Coordinator CS&G

Disposal of Property

No	Reference	Question	Response	Comments	Respondent
1	s3.58(3)	Where the local government disposed of property other than by public auction or tender, did it dispose of the property in accordance with section 3.58(3) of the *Local Government Act 1995* (unless section 3.58(5) applies)?	N/A		Senior Land and Legal Advisor
2	s3.58(4)	Where the local government disposed of property under section 3.58(3) of the *Local Government Act 1995*, did it provide details, as prescribed by section 3.58(4) of the Act, in the required local public notice for each disposal of property?	N/A		Senior Land and Legal Advisor

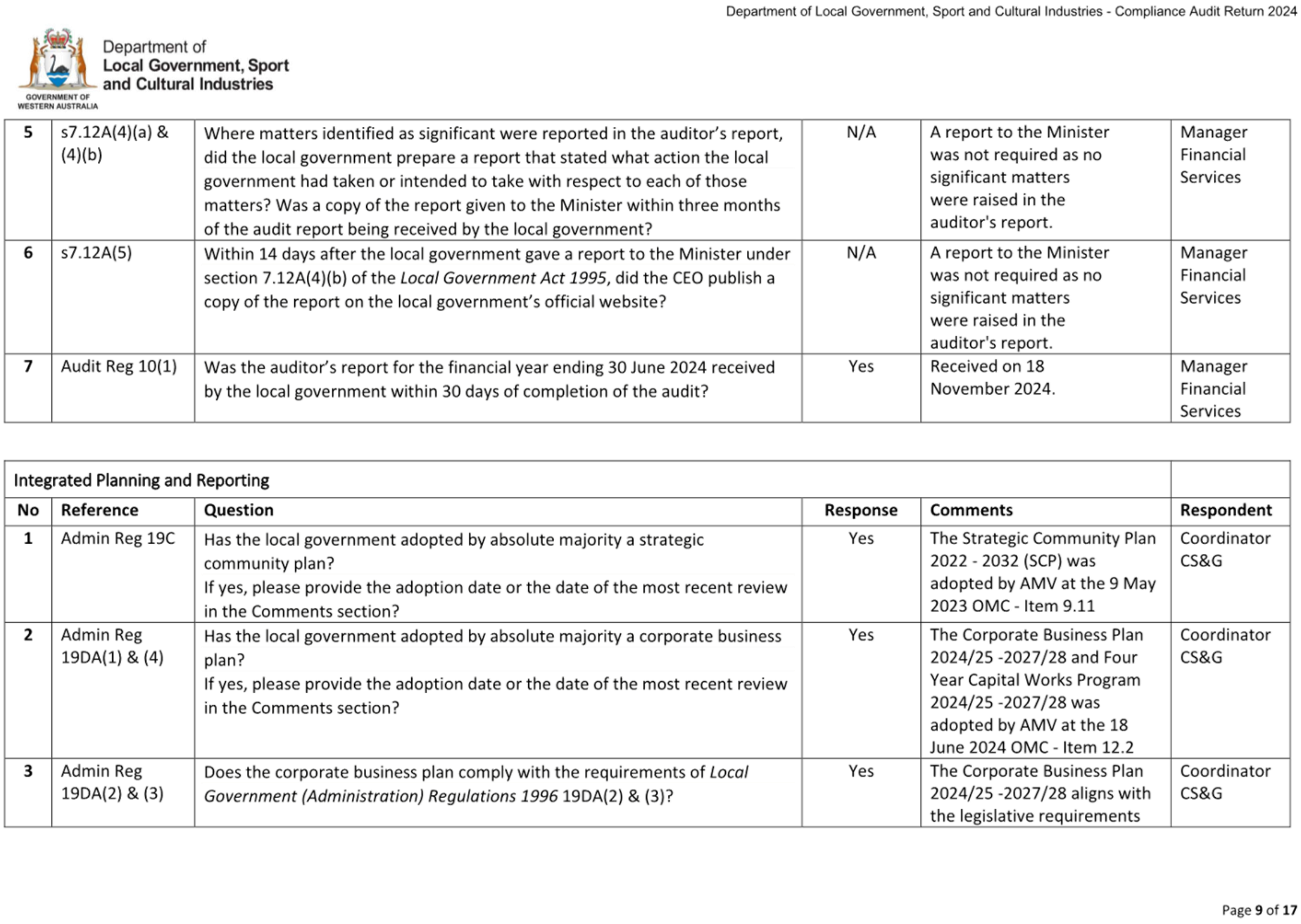
Elections

No	Reference	Question	Response	Comments	Respondent
1	Elect Regs 30G(1) & (2)	Did the CEO establish and maintain an electoral gift register and ensure that all disclosure of gifts forms completed by candidates and donors and received by the CEO were placed on the electoral gift register at the time of receipt by the CEO and in a manner that clearly identifies and distinguishes the forms relating to each candidate in accordance with regulations 30G(1) and 30G(2) of the *Local Government (Elections) Regulations 1997*?	Yes	D23/160848	Executive Assistant to the Mayor & Council Support

Department of
Local Government, Sport and Cultural Industries
GOVERNMENT OF WESTERN AUSTRALIA

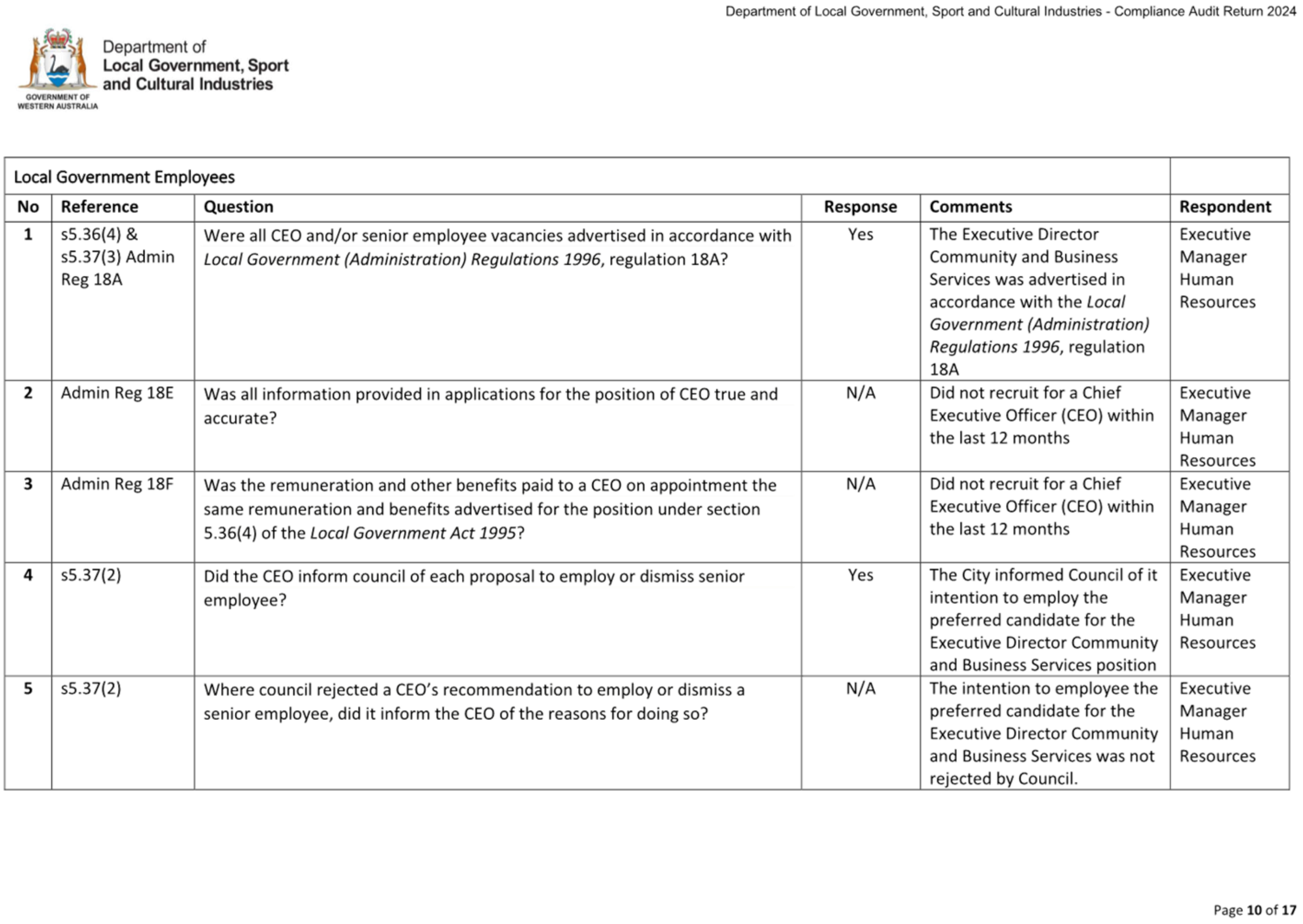
2	Elect Regs 30G(3) & (4)	Did the CEO remove any disclosure of gifts forms relating to an unsuccessful candidate, or a successful candidate that completed their term of office, from the electoral gift register, and retain those forms separately for a period of at least two years in accordance with regulation 30G(4) of the *Local Government (Elections) Regulations 1997*?	N/A		Executive Assistant to the Mayor & Council Support
3	Elect Regs 30G(5) & (6)	Did the CEO publish an up-to-date version of the electoral gift register on the local government's official website in accordance with regulation 30G(5) of the *Local Government (Elections) Regulations 1997*?	Yes	Electoral_Gift_Register_-_2023_2_.pdf	Executive Assistant to the Mayor & Council Support

Finance					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s7.1A	Has the local government established an audit committee and appointed members by absolute majority in accordance with section 7.1A of the *Local Government Act 1995*?	Yes	Appointment of Council Members and Community Representatives by Absolute Majority at Ordinary Council meeting 21 November 2023 – Item 12.2.	Coordinator CS&G
2	s7.1B	Where the council delegated to its audit committee any powers or duties under Part 7 of the *Local Government Act 1995*, did it do so by absolute majority?	N/A	No powers have been delegated to the Audit & Risk Committee.	Coordinator CS&G
3	s7.9(1)	Was the auditor's report for the financial year ended 30 June 2024 received by the local government by 31 December 2024?	Yes	Received on 18 November 2024.	Manager Financial Services
4	s7.12A(3)	Where the local government determined that matters raised in the auditor's report prepared under section 7.9(1) of the *Local Government Act 1995* required action to be taken, did the local government ensure that appropriate action was undertaken in respect of those matters?	Yes	All audit matters raised have appropriate action items and are monitored and tracked by the Audit Committee.	Manager Financial Services



5	s7.12A(4)(a) & (4)(b)	Where matters identified as significant were reported in the auditor's report, did the local government prepare a report that stated what action the local government had taken or intended to take with respect to each of those matters? Was a copy of the report given to the Minister within three months of the audit report being received by the local government?	N/A	A report to the Minister was not required as no significant matters were raised in the auditor's report.	Manager Financial Services
6	s7.12A(5)	Within 14 days after the local government gave a report to the Minister under section 7.12A(4)(b) of the *Local Government Act 1995*, did the CEO publish a copy of the report on the local government's official website?	N/A	A report to the Minister was not required as no significant matters were raised in the auditor's report.	Manager Financial Services
7	Audit Reg 10(1)	Was the auditor's report for the financial year ending 30 June 2024 received by the local government within 30 days of completion of the audit?	Yes	Received on 18 November 2024.	Manager Financial Services

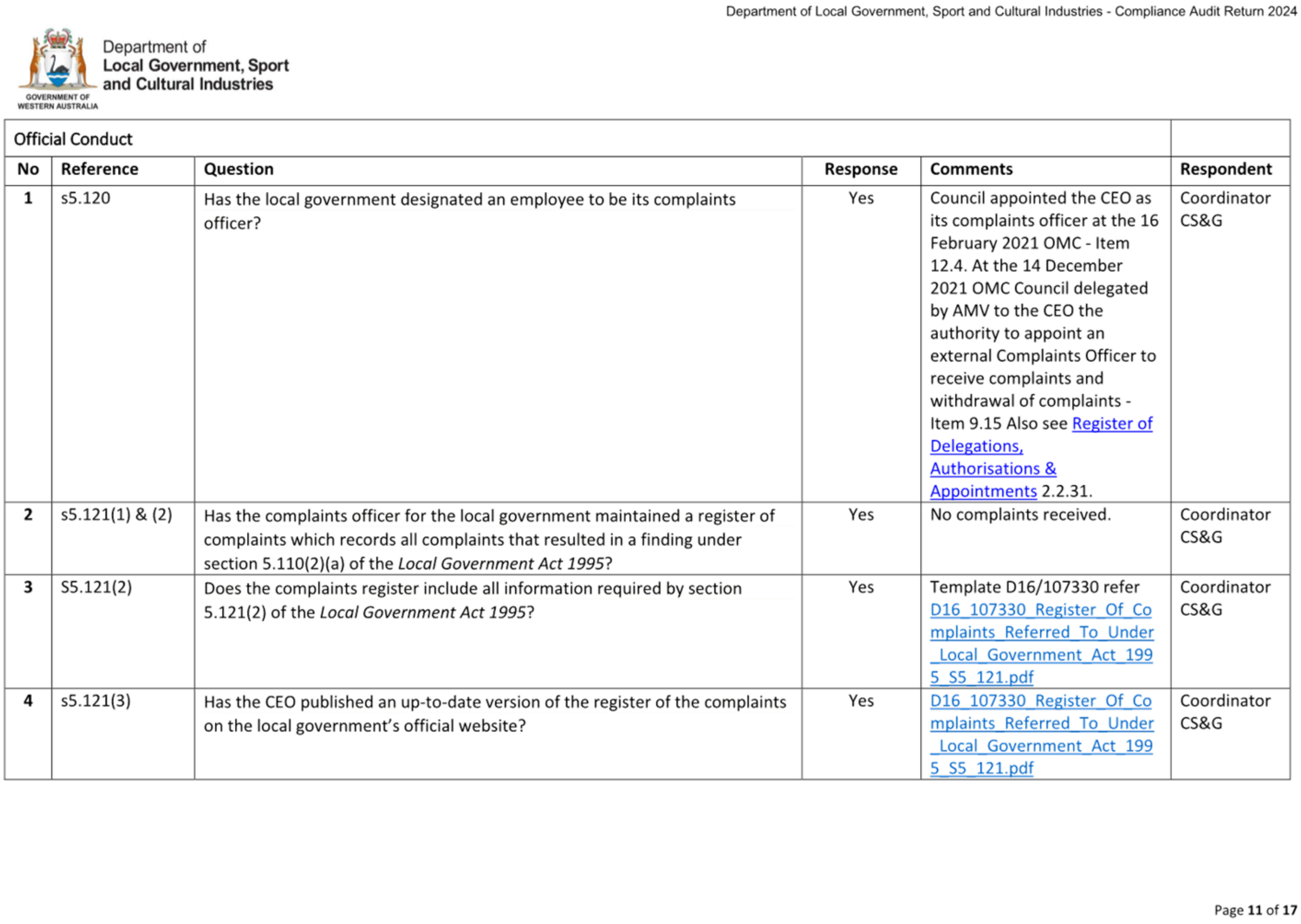
Integrated Planning and Reporting					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	Admin Reg 19C	Has the local government adopted by absolute majority a strategic community plan? If yes, please provide the adoption date or the date of the most recent review in the Comments section?	Yes	The Strategic Community Plan 2022 - 2032 (SCP) was adopted by AMV at the 9 May 2023 OMC - Item 9.11	Coordinator CS&G
2	Admin Reg 19DA(1) & (4)	Has the local government adopted by absolute majority a corporate business plan? If yes, please provide the adoption date or the date of the most recent review in the Comments section?	Yes	The Corporate Business Plan 2024/25 -2027/28 and Four Year Capital Works Program 2024/25 -2027/28 was adopted by AMV at the 18 June 2024 OMC - Item 12.2	Coordinator CS&G
3	Admin Reg 19DA(2) & (3)	Does the corporate business plan comply with the requirements of *Local Government (Administration) Regulations 1996* 19DA(2) & (3)?	Yes	The Corporate Business Plan 2024/25 -2027/28 aligns with the legislative requirements	Coordinator CS&G



GOVERNMENT OF WESTERN AUSTRALIA

Department of
**Local Government, Sport
and Cultural Industries**

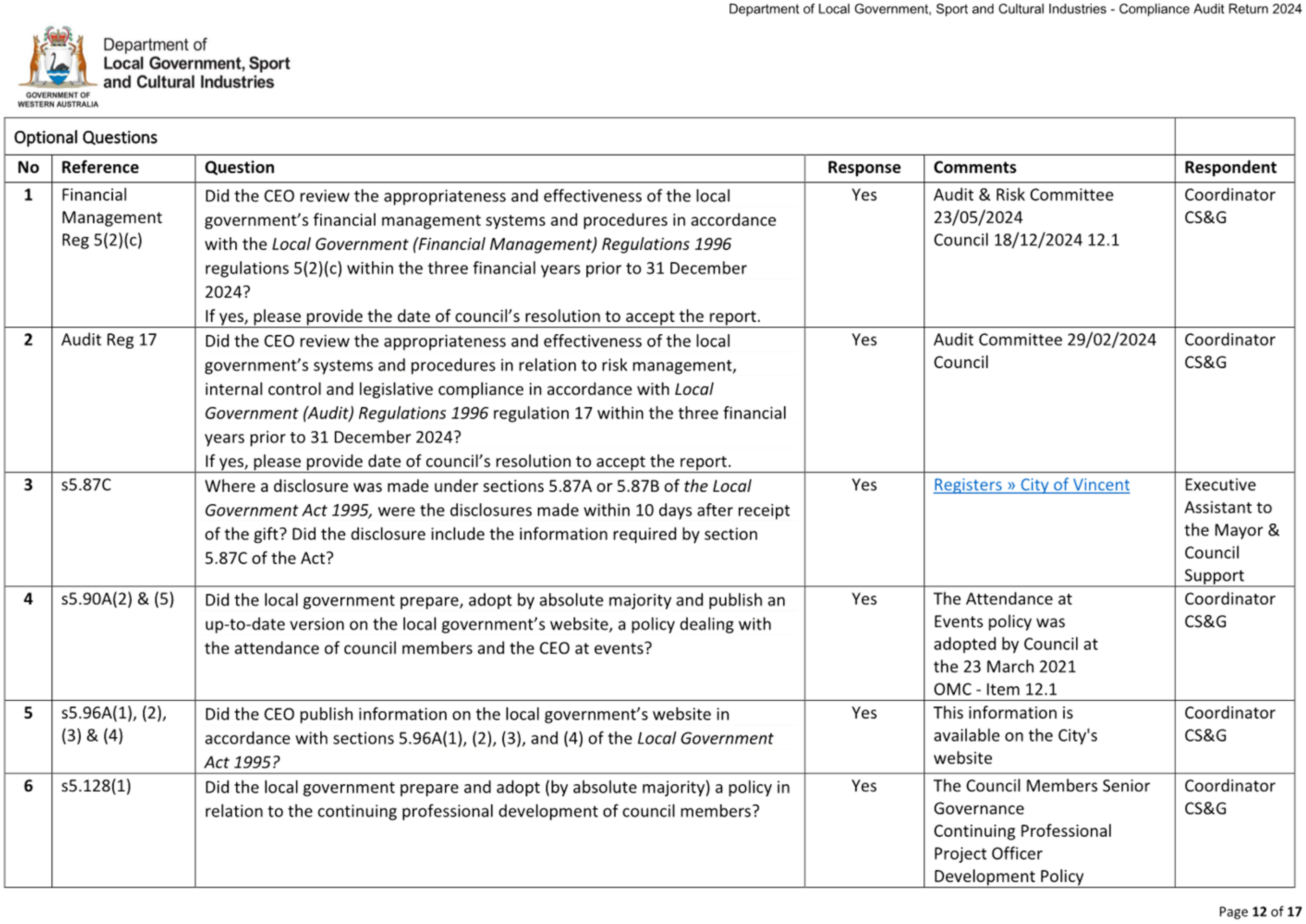
Local Government Employees					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s5.36(4) & s5.37(3) Admin Reg 18A	Were all CEO and/or senior employee vacancies advertised in accordance with *Local Government (Administration) Regulations 1996*, regulation 18A?	Yes	The Executive Director Community and Business Services was advertised in accordance with the *Local Government (Administration) Regulations 1996*, regulation 18A	Executive Manager Human Resources
2	Admin Reg 18E	Was all information provided in applications for the position of CEO true and accurate?	N/A	Did not recruit for a Chief Executive Officer (CEO) within the last 12 months	Executive Manager Human Resources
3	Admin Reg 18F	Was the remuneration and other benefits paid to a CEO on appointment the same remuneration and benefits advertised for the position under section 5.36(4) of the *Local Government Act 1995*?	N/A	Did not recruit for a Chief Executive Officer (CEO) within the last 12 months	Executive Manager Human Resources
4	s5.37(2)	Did the CEO inform council of each proposal to employ or dismiss senior employee?	Yes	The City informed Council of it intention to employ the preferred candidate for the Executive Director Community and Business Services position	Executive Manager Human Resources
5	s5.37(2)	Where council rejected a CEO's recommendation to employ or dismiss a senior employee, did it inform the CEO of the reasons for doing so?	N/A	The intention to employee the preferred candidate for the Executive Director Community and Business Services was not rejected by Council.	Executive Manager Human Resources



GOVERNMENT OF WESTERN AUSTRALIA

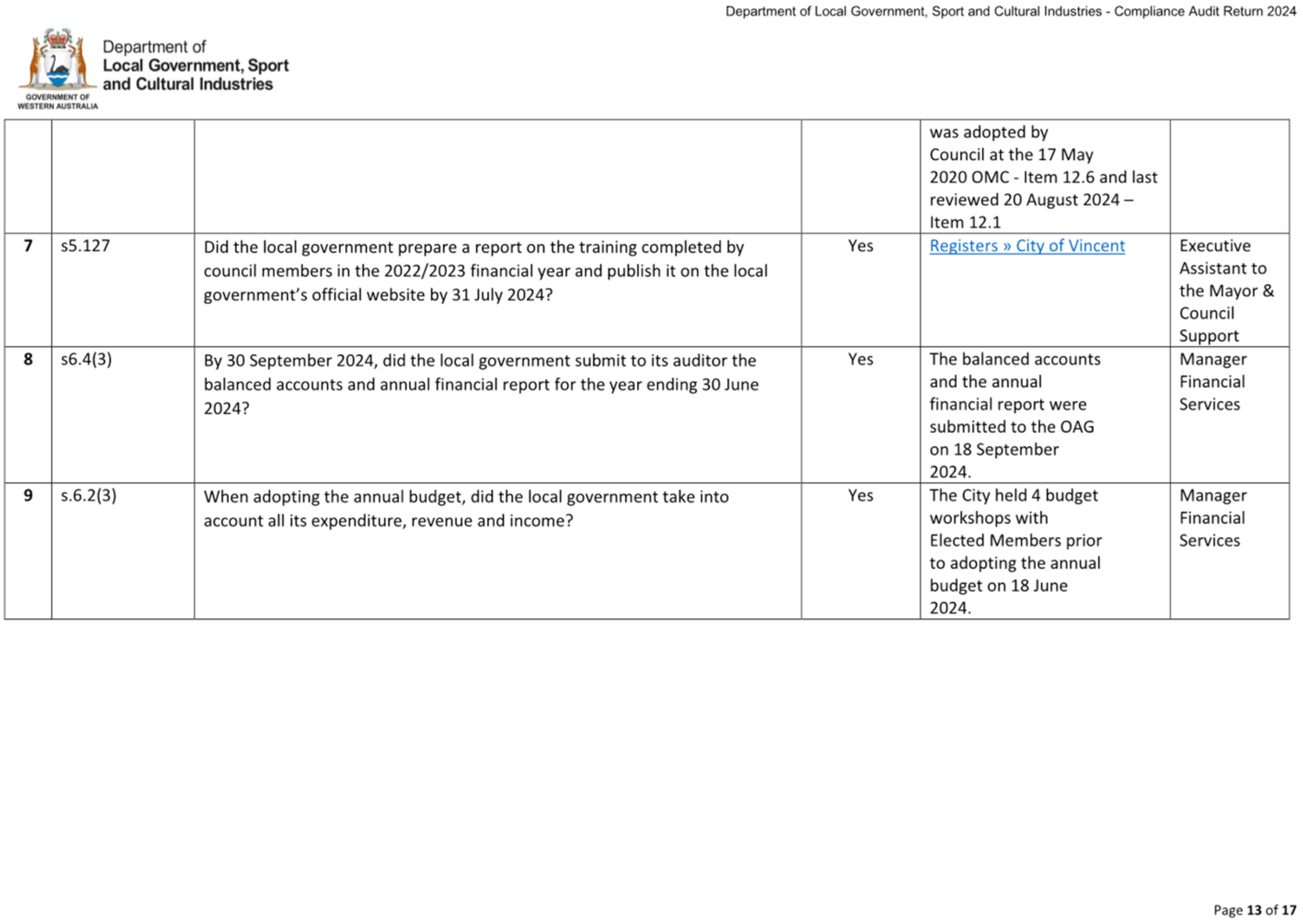
Department of Local Government, Sport and Cultural Industries

Official Conduct					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	s5.120	Has the local government designated an employee to be its complaints officer?	Yes	Council appointed the CEO as its complaints officer at the 16 February 2021 OMC - Item 12.4. At the 14 December 2021 OMC Council delegated by AMV to the CEO the authority to appoint an external Complaints Officer to receive complaints and withdrawal of complaints - Item 9.15 Also see Register of Delegations, Authorisations & Appointments 2.2.31.	Coordinator CS&G
2	s5.121(1) & (2)	Has the complaints officer for the local government maintained a register of complaints which records all complaints that resulted in a finding under section 5.110(2)(a) of the *Local Government Act 1995*?	Yes	No complaints received.	Coordinator CS&G
3	S5.121(2)	Does the complaints register include all information required by section 5.121(2) of the *Local Government Act 1995*?	Yes	Template D16/107330 refer D16_107330_Register_Of_Complaints_Referred_To_Under_Local_Government_Act_1995_S5_121.pdf	Coordinator CS&G
4	s5.121(3)	Has the CEO published an up-to-date version of the register of the complaints on the local government's official website?	Yes	D16_107330_Register_Of_Complaints_Referred_To_Under_Local_Government_Act_1995_S5_121.pdf	Coordinator CS&G



Department of
Local Government, Sport and Cultural Industries
GOVERNMENT OF WESTERN AUSTRALIA

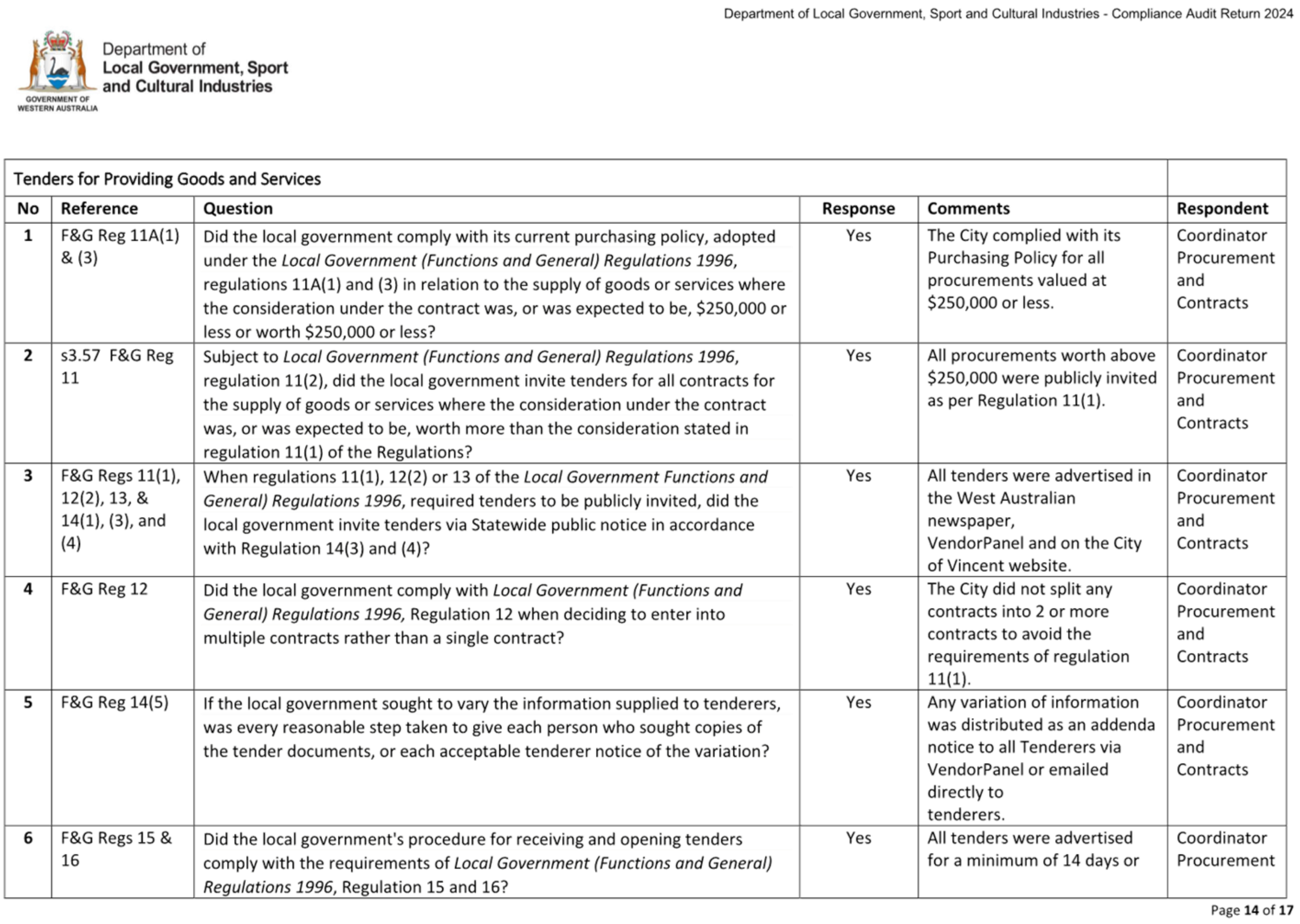
Optional Questions					
No	**Reference**	**Question**	**Response**	**Comments**	**Respondent**
1	Financial Management Reg 5(2)(c)	Did the CEO review the appropriateness and effectiveness of the local government's financial management systems and procedures in accordance with the *Local Government (Financial Management) Regulations 1996* regulations 5(2)(c) within the three financial years prior to 31 December 2024? If yes, please provide the date of council's resolution to accept the report.	Yes	Audit & Risk Committee 23/05/2024 Council 18/12/2024 12.1	Coordinator CS&G
2	Audit Reg 17	Did the CEO review the appropriateness and effectiveness of the local government's systems and procedures in relation to risk management, internal control and legislative compliance in accordance with *Local Government (Audit) Regulations 1996* regulation 17 within the three financial years prior to 31 December 2024? If yes, please provide date of council's resolution to accept the report.	Yes	Audit Committee 29/02/2024 Council	Coordinator CS&G
3	s5.87C	Where a disclosure was made under sections 5.87A or 5.87B of *the Local Government Act 1995,* were the disclosures made within 10 days after receipt of the gift? Did the disclosure include the information required by section 5.87C of the Act?	Yes	Registers » City of Vincent	Executive Assistant to the Mayor & Council Support
4	s5.90A(2) & (5)	Did the local government prepare, adopt by absolute majority and publish an up-to-date version on the local government's website, a policy dealing with the attendance of council members and the CEO at events?	Yes	The Attendance at Events policy was adopted by Council at the 23 March 2021 OMC - Item 12.1	Coordinator CS&G
5	s5.96A(1), (2), (3) & (4)	Did the CEO publish information on the local government's website in accordance with sections 5.96A(1), (2), (3), and (4) of the *Local Government Act 1995?*	Yes	This information is available on the City's website	Coordinator CS&G
6	s5.128(1)	Did the local government prepare and adopt (by absolute majority) a policy in relation to the continuing professional development of council members?	Yes	The Council Members Senior Governance Continuing Professional Project Officer Development Policy	Coordinator CS&G



Department of
Local Government, Sport and Cultural Industries

GOVERNMENT OF WESTERN AUSTRALIA

				was adopted by Council at the 17 May 2020 OMC - Item 12.6 and last reviewed 20 August 2024 – Item 12.1	
7	s5.127	Did the local government prepare a report on the training completed by council members in the 2022/2023 financial year and publish it on the local government's official website by 31 July 2024?	Yes	Registers » City of Vincent	Executive Assistant to the Mayor & Council Support
8	s6.4(3)	By 30 September 2024, did the local government submit to its auditor the balanced accounts and annual financial report for the year ending 30 June 2024?	Yes	The balanced accounts and the annual financial report were submitted to the OAG on 18 September 2024.	Manager Financial Services
9	s.6.2(3)	When adopting the annual budget, did the local government take into account all its expenditure, revenue and income?	Yes	The City held 4 budget workshops with Elected Members prior to adopting the annual budget on 18 June 2024.	Manager Financial Services



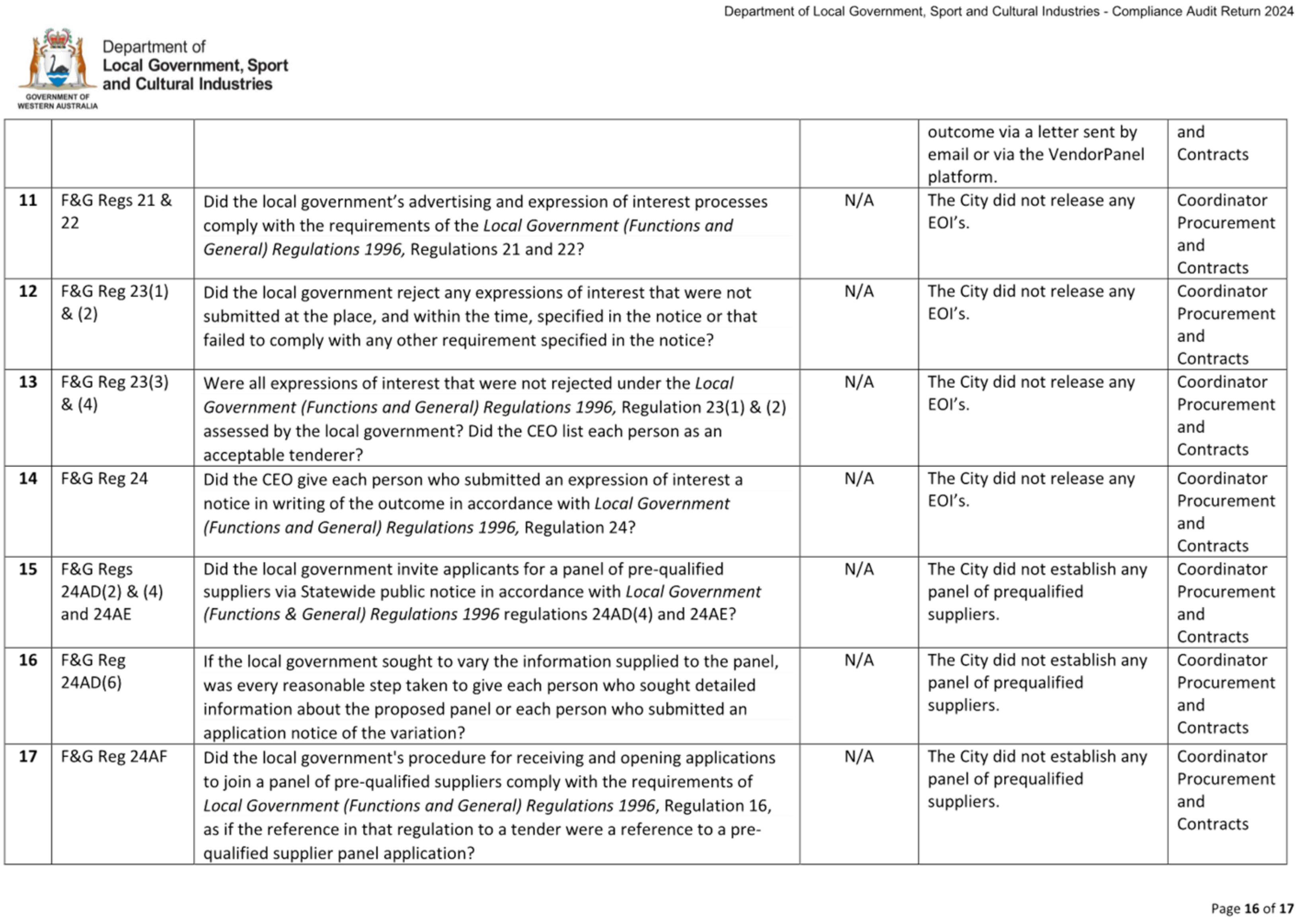
Department of Local Government, Sport and Cultural Industries

GOVERNMENT OF WESTERN AUSTRALIA

Tenders for Providing Goods and Services

No	Reference	Question	Response	Comments	Respondent
1	F&G Reg 11A(1) & (3)	Did the local government comply with its current purchasing policy, adopted under the *Local Government (Functions and General) Regulations 1996*, regulations 11A(1) and (3) in relation to the supply of goods or services where the consideration under the contract was, or was expected to be, $250,000 or less or worth $250,000 or less?	Yes	The City complied with its Purchasing Policy for all procurements valued at $250,000 or less.	Coordinator Procurement and Contracts
2	s3.57 F&G Reg 11	Subject to *Local Government (Functions and General) Regulations 1996*, regulation 11(2), did the local government invite tenders for all contracts for the supply of goods or services where the consideration under the contract was, or was expected to be, worth more than the consideration stated in regulation 11(1) of the Regulations?	Yes	All procurements worth above $250,000 were publicly invited as per Regulation 11(1).	Coordinator Procurement and Contracts
3	F&G Regs 11(1), 12(2), 13, & 14(1), (3), and (4)	When regulations 11(1), 12(2) or 13 of the *Local Government Functions and General) Regulations 1996*, required tenders to be publicly invited, did the local government invite tenders via Statewide public notice in accordance with Regulation 14(3) and (4)?	Yes	All tenders were advertised in the West Australian newspaper, VendorPanel and on the City of Vincent website.	Coordinator Procurement and Contracts
4	F&G Reg 12	Did the local government comply with *Local Government (Functions and General) Regulations 1996,* Regulation 12 when deciding to enter into multiple contracts rather than a single contract?	Yes	The City did not split any contracts into 2 or more contracts to avoid the requirements of regulation 11(1).	Coordinator Procurement and Contracts
5	F&G Reg 14(5)	If the local government sought to vary the information supplied to tenderers, was every reasonable step taken to give each person who sought copies of the tender documents, or each acceptable tenderer notice of the variation?	Yes	Any variation of information was distributed as an addenda notice to all Tenderers via VendorPanel or emailed directly to tenderers.	Coordinator Procurement and Contracts
6	F&G Regs 15 & 16	Did the local government's procedure for receiving and opening tenders comply with the requirements of *Local Government (Functions and General) Regulations 1996*, Regulation 15 and 16?	Yes	All tenders were advertised for a minimum of 14 days or	Coordinator Procurement

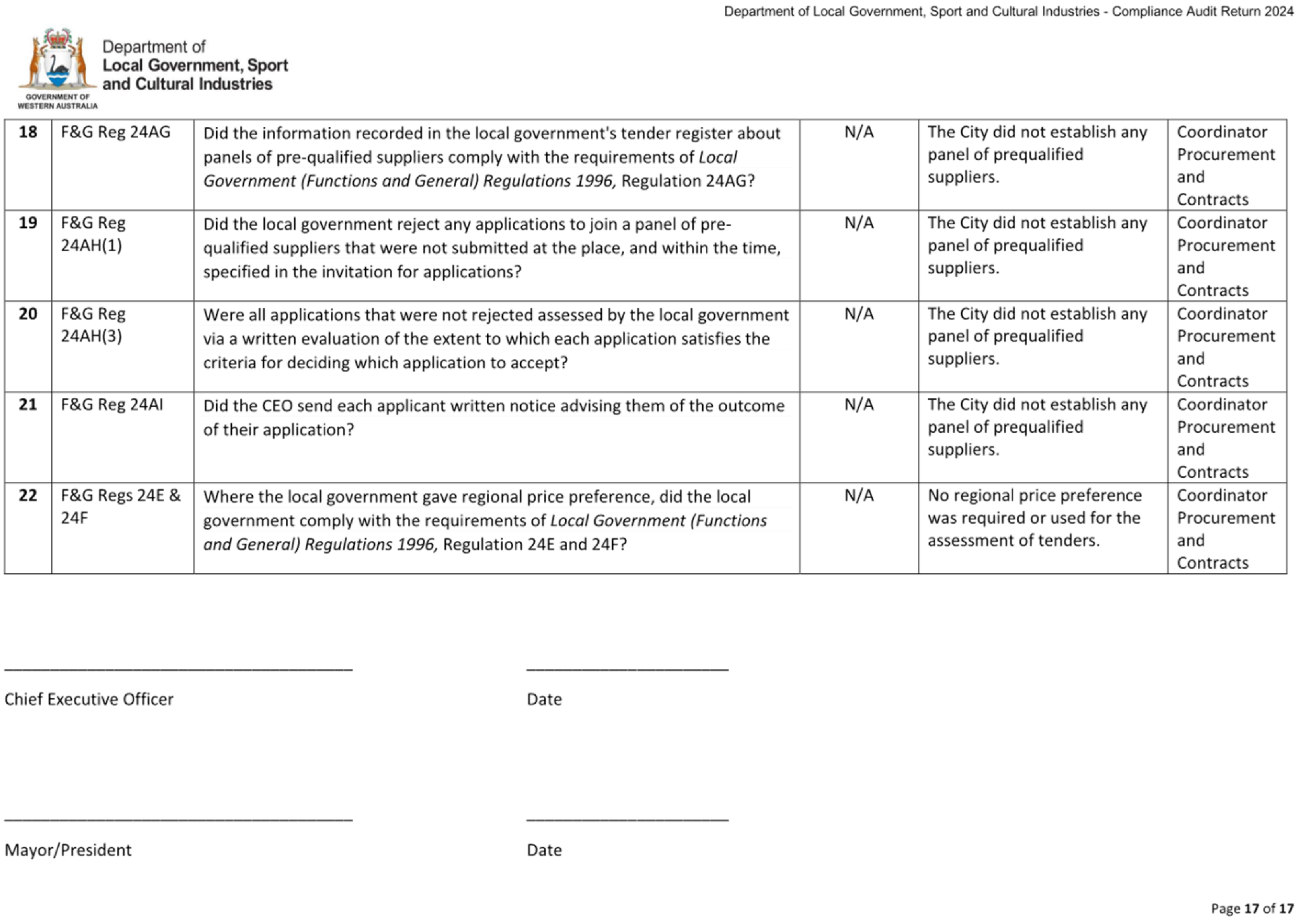
				more as required under Regulation 15. Two City officers were always present when tenders were opened. Tenders were opened in a public place as published in the relevant request for tender document.	and Contracts
7	F&G Reg 17	Did the information recorded in the local government's tender register comply with the requirements of the *Local Government (Functions and General) Regulations 1996*, Regulation 17 and did the CEO make the tenders register available for public inspection and publish it on the local government's official website?	Yes	All information recorded in the tender register complied with Regulation 17. The City's tender register is published on the City's official website and is publicly available.	Coordinator Procurement and Contracts
8	F&G Reg 18(1)	Did the local government reject any tenders that were not submitted at the place, and within the time, specified in the invitation to tender?	Yes	The City used VendorPanel for all tenders. Any tender not submitted through VendorPanel or within the time and date specified in the tender were rejected. The City does not accept hardcopy tenders and VendorPanel does not allow tender responses to be submitted after the closing time and date.	Coordinator Procurement and Contracts
9	F&G Reg 18(4)	Were all tenders that were not rejected assessed by the local government via a written evaluation of the extent to which each tender satisfies the criteria for deciding which tender to accept?	Yes	All compliant tenders were evaluated by an evaluation panel and evaluation reports were generated and approved as per the City's Purchasing Policy.	Coordinator Procurement and Contracts
10	F&G Reg 19	Did the CEO give each tenderer written notice containing particulars of the successful tender or advising that no tender was accepted?	Yes	All tender respondents were notified of the evaluation	Coordinator Procurement



Department of
Local Government, Sport and Cultural Industries

GOVERNMENT OF WESTERN AUSTRALIA

				outcome via a letter sent by email or via the VendorPanel platform.	and Contracts
11	F&G Regs 21 & 22	Did the local government's advertising and expression of interest processes comply with the requirements of the *Local Government (Functions and General) Regulations 1996,* Regulations 21 and 22?	N/A	The City did not release any EOI's.	Coordinator Procurement and Contracts
12	F&G Reg 23(1) & (2)	Did the local government reject any expressions of interest that were not submitted at the place, and within the time, specified in the notice or that failed to comply with any other requirement specified in the notice?	N/A	The City did not release any EOI's.	Coordinator Procurement and Contracts
13	F&G Reg 23(3) & (4)	Were all expressions of interest that were not rejected under the *Local Government (Functions and General) Regulations 1996,* Regulation 23(1) & (2) assessed by the local government? Did the CEO list each person as an acceptable tenderer?	N/A	The City did not release any EOI's.	Coordinator Procurement and Contracts
14	F&G Reg 24	Did the CEO give each person who submitted an expression of interest a notice in writing of the outcome in accordance with *Local Government (Functions and General) Regulations 1996,* Regulation 24?	N/A	The City did not release any EOI's.	Coordinator Procurement and Contracts
15	F&G Regs 24AD(2) & (4) and 24AE	Did the local government invite applicants for a panel of pre-qualified suppliers via Statewide public notice in accordance with *Local Government (Functions & General) Regulations 1996* regulations 24AD(4) and 24AE?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
16	F&G Reg 24AD(6)	If the local government sought to vary the information supplied to the panel, was every reasonable step taken to give each person who sought detailed information about the proposed panel or each person who submitted an application notice of the variation?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
17	F&G Reg 24AF	Did the local government's procedure for receiving and opening applications to join a panel of pre-qualified suppliers comply with the requirements of *Local Government (Functions and General) Regulations 1996*, Regulation 16, as if the reference in that regulation to a tender were a reference to a pre-qualified supplier panel application?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts



18	F&G Reg 24AG	Did the information recorded in the local government's tender register about panels of pre-qualified suppliers comply with the requirements of *Local Government (Functions and General) Regulations 1996,* Regulation 24AG?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
19	F&G Reg 24AH(1)	Did the local government reject any applications to join a panel of pre-qualified suppliers that were not submitted at the place, and within the time, specified in the invitation for applications?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
20	F&G Reg 24AH(3)	Were all applications that were not rejected assessed by the local government via a written evaluation of the extent to which each application satisfies the criteria for deciding which application to accept?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
21	F&G Reg 24AI	Did the CEO send each applicant written notice advising them of the outcome of their application?	N/A	The City did not establish any panel of prequalified suppliers.	Coordinator Procurement and Contracts
22	F&G Regs 24E & 24F	Where the local government gave regional price preference, did the local government comply with the requirements of *Local Government (Functions and General) Regulations 1996,* Regulation 24E and 24F?	N/A	No regional price preference was required or used for the assessment of tenders.	Coordinator Procurement and Contracts

________________________________ ____________________

Chief Executive Officer Date

________________________________ ____________________

Mayor/President Date

5.5 CYBER-SECURITY CONTROLS REVIEW 2024 FROM JLT PUBLIC SECTOR

Attachments: 1. LGIS Vincent City of Cyber Review 2024 - Confidential

RECOMMENDATION:

That the Audit Committee recommends to Council that it NOTES the JLT Public Sector's report on the City's cyber security controls.

<u>COMMITTEE DECISION ITEM 5.5</u>

<u>Moved:</u> Mr Isambert, <u>Seconded:</u> Cr Hallett

That the recommendation be adopted.

<u>CARRIED (6-0)</u>

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

5.6 REVIEW OF THE CITY'S CORPORATE RISK REGISTER

Attachments:

1. **Corporate Risk Register - Confidential**
2. **Risk Management Procedure** ⇩
3. **Risk Appetite and Tolerance Statements** ⇩
4. **Risk Rating Alignment to Appetite and Tolerance** ⇩

RECOMMENDATION:

That the Audit Committee recommends to Council that it:

1. **RECEIVES the City’s Corporate Risk Register at Attachment 1; and**

2. **APPROVES the risk management actions for the high and extreme risks; and**

3. **NOTES alignment of Corporate Risks to risk appetite and tolerance ratings**

COMMITTEE DECISION ITEM 5.6

Moved: Cr Castle, Seconded: Mr Manifis

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

NOTE: The Audit & Risk Committee requested Administration to conduct a deep dive into the tree canopy risk, including the impact of climate change and strategies to meet canopy coverage targets. To be presented to the July meeting.

CITY OF VINCENT

RISK MANAGEMENT PROCEDURE

Responsible directorate	Office of the CEO.
Responsible team	Corporate Strategy and Governance.
Responsible officer	Executive Manager, Corporate Strategy and Governance.
Affected teams	All Staff.
Legislation / local law requirements	Regulation 17 *Local Government (Audit) Regulations 1996.*
Relevant delegations	Nil.
Related policy procedures and documents	This document supports the Risk Management Policy by further defining the systems and processes in place to facilitate good practice risk management.

PURPOSE

To set out the framework within which the City of Vincent (**City**) will manage its strategic, operational and project risks.

BACKGROUND

The City has a Risk Management Policy (**Policy**) approved by Council (16 June 2020 Council Meeting). The Policy sets the tone for the City's risk management approach and establishes the risk management responsibilities of Council, the Audit Committee, City employees and contractors and other relevant parties as required.

This Procedure supports the Policy by defining the systems and processes in place to facilitate good practice risk management and the roles and responsibilities of City employees.

PROCEDURE

1. RISK MANAGEMENT APPROACH

The City's approach to risk management determines how the City will go about managing its risks.

The City's risk management approach aligns with the *AS31000:2018 Risk Management – Guidelines.*

2. OTHER RISK DOCUMENTS

Corporate Risk Register

The Corporate Risk Register (**Register**) lists the City's 'whole of organisation' strategic, operational and project risks. The risks are assessed without controls (*i.e. inherently*), with controls (*i.e. residually*) and following the proposed risk management actions (*i.e. post-treatment*).

The Register is divided into a list of residually-rated medium, high and extreme risks (which require reporting to the Executive Management Committee, Audit Committee and Council) and residually-rated low and medium risks for each service area. Timeframes and ownership for the implementation of the risk management actions are included.

Risk Appetite and Tolerance Statements

'Risk Appetite' sets out the risk type and levels that the City is looking to pursue to meet and optimise opportunities. 'Risk Tolerance' reflects how much risk the City is able to accept in the pursuit of its strategic, operational and project objectives.

Strategy House Service Area Risk Matrix

Each of the City's service areas has a risk matrix which sets out its strategic (where relevant), operational and project risks which are specifically considered, where appropriate, within the context of the specific Strategy House.

A number of documents and guidelines are also relevant to the City's risk management. These include:

- *Business continuity plan (BCP)* – This document describes how the City will respond to and function in the event of a business interruption event. It is a 'mitigative' control as it seeks to reduce the consequences of risks eventuating.
- *ICT disaster recovery plans* – these plans assist the City to recover from Information and Communication Technology (**ICT**) interruption events, from a routine, operational incident through to a large-scale ICT event. The plans will ultimately align with the City's BCP and, again, are 'mitigative' controls in seeking to reduce the consequence of a risk eventuating.
- *Event risk management plans* – These are formal plans to mitigate any foreseeable risks that may arise from place activation, and planning and delivering events.
- *Procurement risk assessments* – A systematic, documented assessment of risks associated with all significant purchases, as set out in the Procurement Plan. Procurement risk assessments are required for procurement of greater than $50,000, and the level of detail required for the risk assessment will vary depending on the significance of the purchase. Note that although the $50,000 mandatory threshold has been set by the City, the contract value of a procurement does not define its

risk to the City so there is discretion – which should be exercised – in contract values below this figure.

3. RISK CATEGORIES

Strategic Risks

Strategic risks relate to the uncertainty of the City achieving its long-term, strategic objectives. They are usually owned and managed by Council and/or the Executive Management Committee. Strategic level risks may include risks associated with achieving the objectives of the Strategic Community Plan, Corporate Business Plan and the Long-Term Financial Plan.

Operational Risks

Operational risks relate to the uncertainty associated with developing or delivering the City's services, functions and other activities. These risks typically have day to day impacts on the organisation or more widely. These risks are owned and managed by the person who has responsibility for the activity, service or function to the level of their delegated authority or capability.

Project Risks

Project risks typically sit underneath operational risks and will be managed in accordance with the City's Project Management Framework and depending on their progress.

4. RISK MANAGEMENT PROCESS

Step 1 - Establishing the scope, context and criteria

Prior to commencing risk management, the context for the activity is clearly specified. This includes defining:

- the purpose of the risk exercise and the expected outcomes;
- the scope, boundaries, assumptions and interrelationships;
- the environment, objective, strategy, activity, process, function, project, product, service or asset under consideration; and
- the risk assessment methodologies or approach.

Once this is determined, the essential personnel who need to be involved in the assessment are identified.

Step 2 - Risk Assessment

A. Risk Identification

The context defined in the previous step is used as the starting point for identifying risks. A practical and effective approach to risk identification is to consider what is critical to the successful achievement of the objectives related to that particular context, and what are the potential opportunities or 'roadblocks' arising from areas of uncertainty (*e.g. assumptions, limitations, external factors, etc*). Included in this consideration are any internal or external events or situations which may give rise to a risk, and also any risks identified through internal or third-party audits, assessments and reviews. Typically, risks are worded either with the use of '*critical success factors*' (**CSFs**) or through '*cause-event-consequence*' (**CEC**) statements:

1) **CSFs -** When considering an activity, consider what is critical that you get right about the activity (*e.g. with City reporting, it may be timeliness and accuracy*), and word the risk based on this critical activity (*e.g. failure to ensure timely and accurate City reporting*);

2) **CECs -** Consider the event that you are most concerned about (*e.g. timely reporting*), the principal potential cause (*e.g. Inadequate reporting systems*) and the principal potential consequence (*e.g. sub-optimal decision making*). These can then be constructed into a statement (*e.g. Inadequate systems cause untimely reporting leading to suboptimal decision making*).

Both ways of phrasing risks are acceptable to the City. Each risk requires a risk owner who is responsible for managing the risk and is accountable for determining if the risk level can be accepted, reviewing the risk, monitoring the controls and risk treatments. High and extreme risks require the risk management action to be approved by Council, via the Audit Committee.

B. Risk analysis and evaluation

For each risk, possible causes of the risk eventuating are identified. Each risk may have one or more causal factors which can either directly or indirectly contribute to it occurring. Identifying the range of causes assists in understanding the risk, identifying the most appropriate controls, evaluating the adequacy of existing controls and designing effective risk treatments. This step also considers the potential consequences of the risk, including knock-on or cascading effects.

Comparing the level of risk with the contents of the risk assessment criteria determines the acceptability of the risk. Risk analysis is undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis is qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances. Such techniques are comprehensively considered in 'ISO 31010: Risk Assessment Techniques', a companion to AS ISO 31000:2018. Risk analysis and evaluation involves identifying and evaluating any existing controls and analysing the risk in terms of consequences and likelihood, taking into account the effectiveness of the controls (*i.e. 'Residual Risk'*). Understanding the following terms is key:

- Controls - Controls are the measures that are currently in place (*i.e. at the time of the risk assessment*), that materially reduce the consequences and/or likelihood of the risk. Controls are tangible, auditable and documented. A 'Hierarchy of Control' is applied which ensures the most effective controls are considered first (*e.g. eliminate entirely, substitute it, isolate it and engineer it out prior to relying on administrative controls*). At the City, controls are considered to be either 'preventative' (i.e. affecting likelihood), 'mitigative' (i.e. affecting consequence) or both.
- Consequence - A risk that eventuates may impact the City to a greater or lesser extent across multiple areas. Consequences of the risk can be assessed across the relevant consequence categories, which are defined in the risk assessment criteria tables.
- Likelihood - This describes how likely it is that a risk will eventuate with the defined consequences. Likelihood can be assessed in terms of terms of probability or frequency, depending on what is most appropriate for the risk under consideration. When you are rating the likelihood of residual risk, ask "*How likely is it for this risk to occur, given the existing controls, to the level of consequence identified?*"
- Level of Risk - The Level of Risk (LoR), or Risk Rating, is calculated by multiplying the consequence and likelihood ratings. For any risk, there may be a number of different consequence/ likelihood scenarios. Within each category there may be multiple scenarios ranging from 'minor but likely' to 'catastrophic but rare'. The City expects the most realistic worst-case scenario to be rated. In some instances, it may be appropriate to rate the same consequence category more than once. Where there are multiple ratings for a risk, the highest combination of consequence/likelihood is taken as the LoR. The LoR is then compared to the defined risk criteria to assist the risk owner in determining whether a risk requires further treatment. The City captures three different 'Levels of Risk' – Inherent risk (*i.e. before controls are applied*), Residual risk (*i.e. after controls are applied*) and 'Post-treatment' (*i.e. a prospective level of risk considering further treatments*).

Step 3 - Risk Treatment

Once a risk has been analysed and evaluated, the risk owner makes an informed decision to do one of the following:

- Accept the risk – the opportunity outweighs the risk, the existing controls meet the criteria specified in the Risk Assessment Criteria and the risk is within the defined tolerance and appetite of the City;
- Avoid the risk – do not carry on with the activity that is associated with the risk;
- Treat the risk – reduce the consequence, likelihood or both and/or improve the controls rating by strengthening existing controls or developing new controls so that the risk can be accepted. The treatment selection and implementation will typically be based on financial, technical and operational

- viability and alignment to the City's values and objectives. Note: It is expected that any risks associated with health and safety are managed to a level which the City considers to be "as low as reasonably practicable" (ALARP).

Risk-based decisions are made in line with the criteria outlined in the risk assessment criteria tables.

Communication and consultation with external and internal stakeholders/interested parties is an essential and valuable part of the risk management process at the City. A collaborative approach is preferred as it provides the opportunity for different perspectives and expertise. The City has an expectation this will occur throughout the steps 1 to 3 documented. Communication and consultation should include, amongst others, staff of the City, Councillors, contractors, rate payers and residents. Some of this consultation and communication will be formalised through workshops and training and some – for example with ratepayers and residents – may be less formal. Risk management training will be provided to staff, commencing at induction. In addition, regular risk management awareness information will be communicated via the Vintranet.

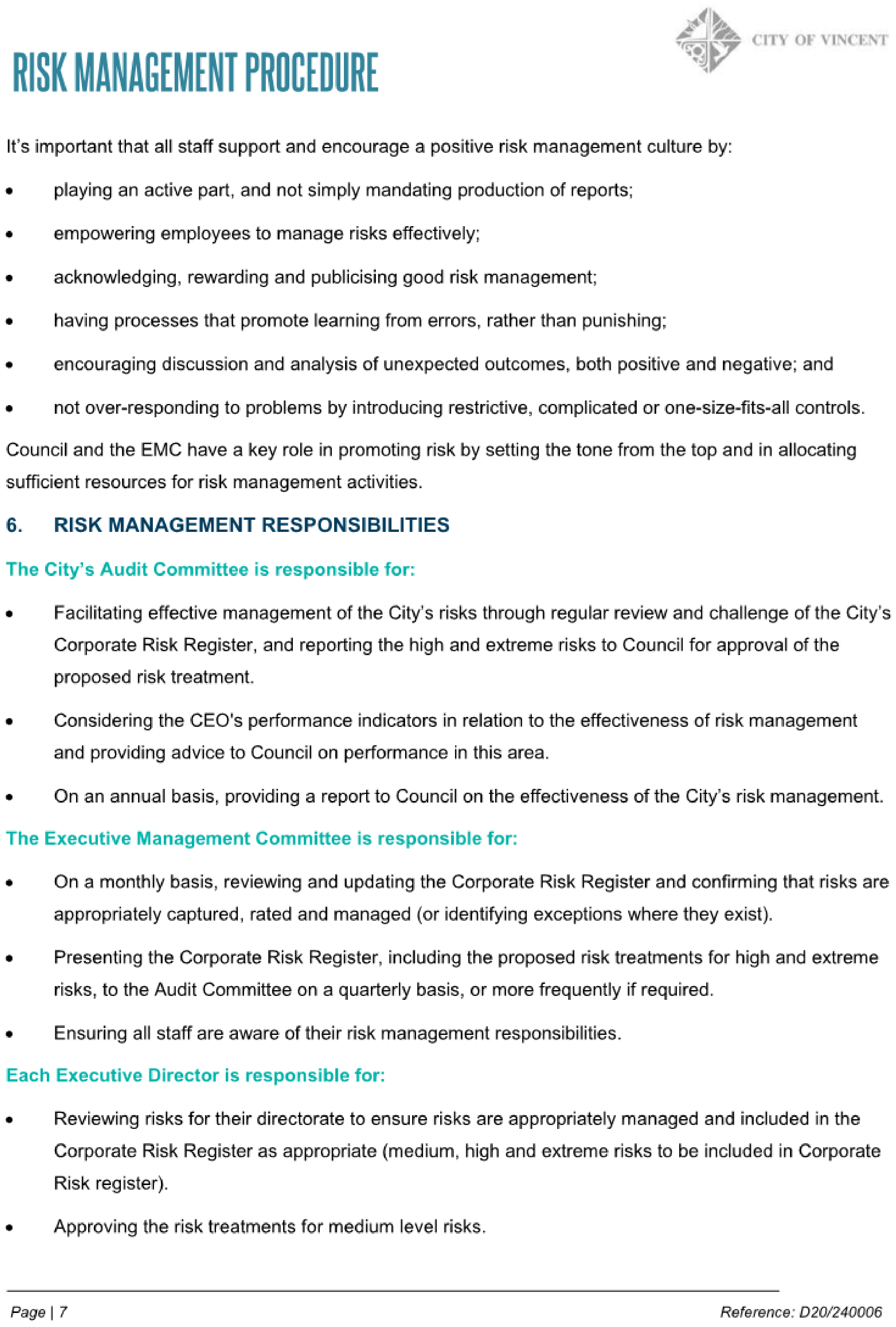
Monitoring and Review and Recording & Reporting are considered integral parts of the planning, management and oversight activities of the City to ensure contemporary, relevant and evidential risk management. The Corporate Risk Register is updated as risks are identified and is reported to the Executive Management Committee monthly, and to the Audit Committee quarterly or more frequently as required.

Ad-hoc review of risks may also occur where:

- There is a change to the risk environment, for example, changes to legislation or to the SCP or the CBP;
- An internal audit or other review highlights a new or changed risk;
- A material risk treatment is implemented or a key control is considered no longer effective or adequate;
- Major changes are made to the organisation including change of key personnel; or
- The complaints or learnings in relation to processes indicate a new or changed risk to the City.

5. RISK MANAGEMENT CULTURE

A risk aware culture is essential to good risk management. The Policy and this Procedure will be communicated across the organisation and embedded into practices and processes rather than be viewed or practiced as a separate activity.



It's important that all staff support and encourage a positive risk management culture by:

- playing an active part, and not simply mandating production of reports;
- empowering employees to manage risks effectively;
- acknowledging, rewarding and publicising good risk management;
- having processes that promote learning from errors, rather than punishing;
- encouraging discussion and analysis of unexpected outcomes, both positive and negative; and
- not over-responding to problems by introducing restrictive, complicated or one-size-fits-all controls.

Council and the EMC have a key role in promoting risk by setting the tone from the top and in allocating sufficient resources for risk management activities.

6. RISK MANAGEMENT RESPONSIBILITIES

The City's Audit Committee is responsible for:

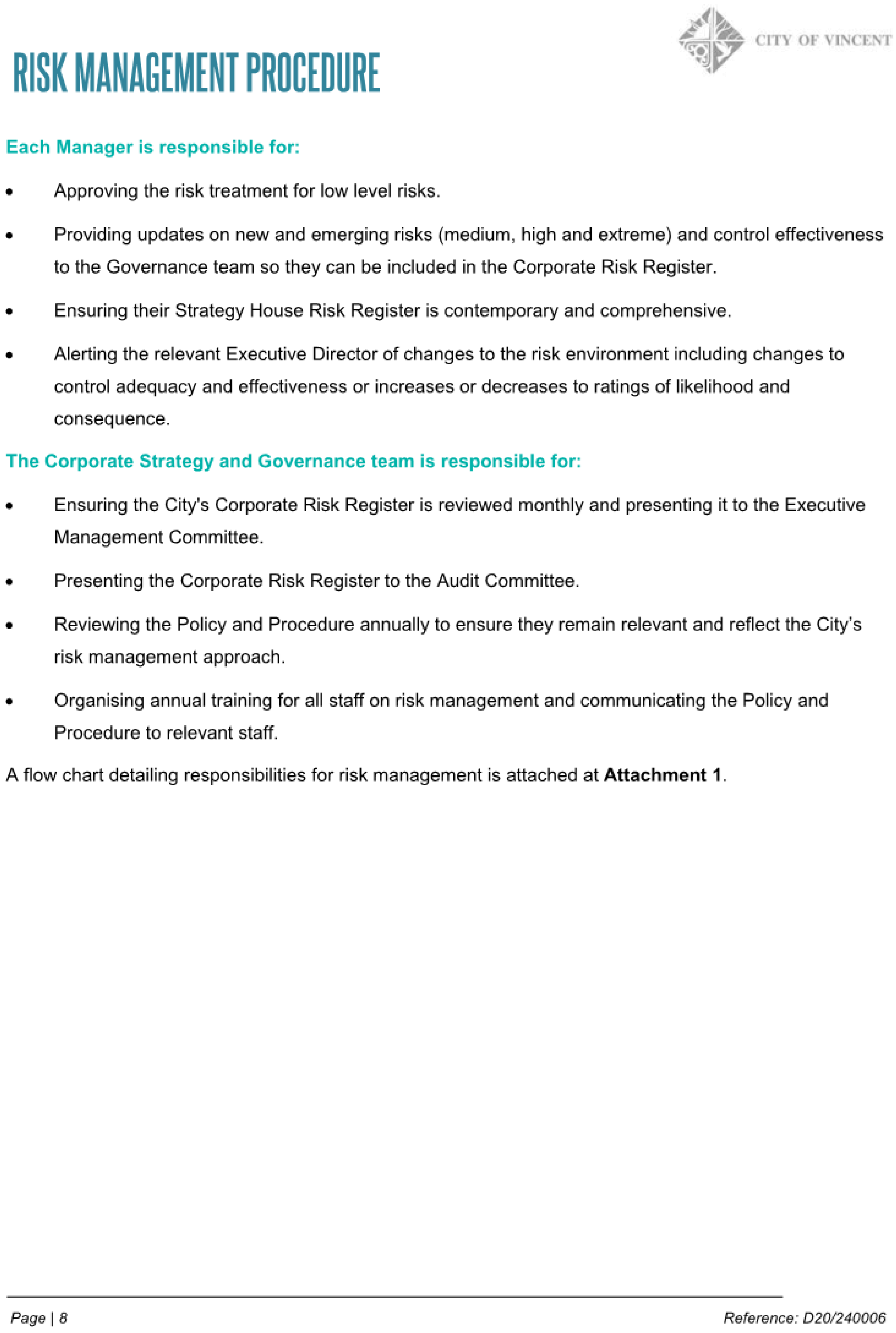
- Facilitating effective management of the City's risks through regular review and challenge of the City's Corporate Risk Register, and reporting the high and extreme risks to Council for approval of the proposed risk treatment.
- Considering the CEO's performance indicators in relation to the effectiveness of risk management and providing advice to Council on performance in this area.
- On an annual basis, providing a report to Council on the effectiveness of the City's risk management.

The Executive Management Committee is responsible for:

- On a monthly basis, reviewing and updating the Corporate Risk Register and confirming that risks are appropriately captured, rated and managed (or identifying exceptions where they exist).
- Presenting the Corporate Risk Register, including the proposed risk treatments for high and extreme risks, to the Audit Committee on a quarterly basis, or more frequently if required.
- Ensuring all staff are aware of their risk management responsibilities.

Each Executive Director is responsible for:

- Reviewing risks for their directorate to ensure risks are appropriately managed and included in the Corporate Risk Register as appropriate (medium, high and extreme risks to be included in Corporate Risk register).
- Approving the risk treatments for medium level risks.



CITY OF VINCENT

RISK MANAGEMENT PROCEDURE

Each Manager is responsible for:

- Approving the risk treatment for low level risks.
- Providing updates on new and emerging risks (medium, high and extreme) and control effectiveness to the Governance team so they can be included in the Corporate Risk Register.
- Ensuring their Strategy House Risk Register is contemporary and comprehensive.
- Alerting the relevant Executive Director of changes to the risk environment including changes to control adequacy and effectiveness or increases or decreases to ratings of likelihood and consequence.

The Corporate Strategy and Governance team is responsible for:

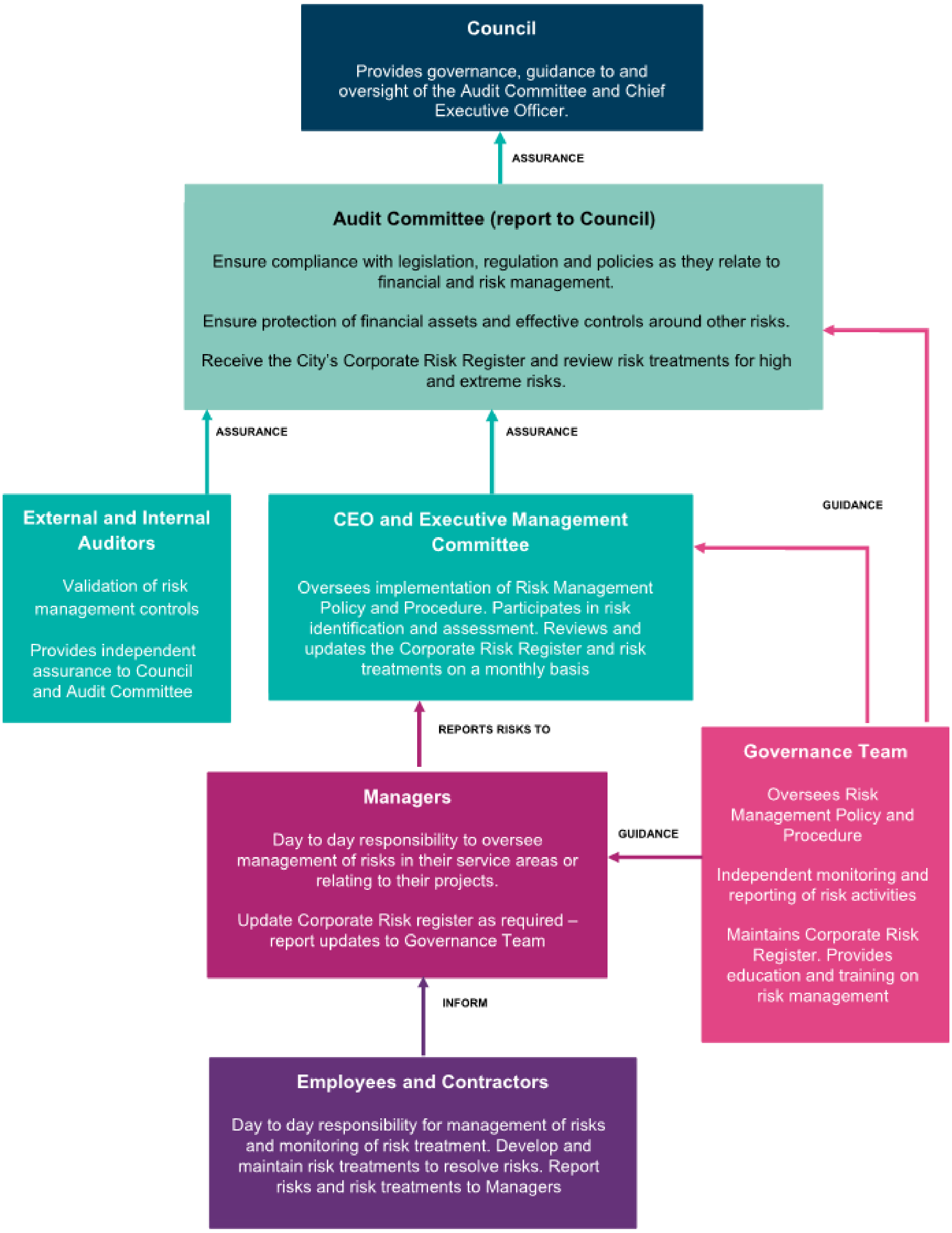
- Ensuring the City's Corporate Risk Register is reviewed monthly and presenting it to the Executive Management Committee.
- Presenting the Corporate Risk Register to the Audit Committee.
- Reviewing the Policy and Procedure annually to ensure they remain relevant and reflect the City's risk management approach.
- Organising annual training for all staff on risk management and communicating the Policy and Procedure to relevant staff.

A flow chart detailing responsibilities for risk management is attached at **Attachment 1**.

CITY OF VINCENT

RISK MANAGEMENT PROCEDURE

ATTACHMENT 1 – RISK RESPONSIBILITY



Council

Provides governance, guidance to and oversight of the Audit Committee and Chief Executive Officer.

Audit Committee (report to Council)

Ensure compliance with legislation, regulation and policies as they relate to financial and risk management.

Ensure protection of financial assets and effective controls around other risks.

Receive the City's Corporate Risk Register and review risk treatments for high and extreme risks.

External and Internal Auditors

Validation of risk management controls

Provides independent assurance to Council and Audit Committee

CEO and Executive Management Committee

Oversees implementation of Risk Management Policy and Procedure. Participates in risk identification and assessment. Reviews and updates the Corporate Risk Register and risk treatments on a monthly basis

Governance Team

Oversees Risk Management Policy and Procedure

Independent monitoring and reporting of risk activities

Maintains Corporate Risk Register. Provides education and training on risk management

Managers

Day to day responsibility to oversee management of risks in their service areas or relating to their projects.

Update Corporate Risk register as required – report updates to Governance Team

Employees and Contractors

Day to day responsibility for management of risks and monitoring of risk treatment. Develop and maintain risk treatments to resolve risks. Report risks and risk treatments to Managers

OFFICE USE ONLY	
Approved by CEO and Noted by Audit Committee	DATE: 06/07/2021, REF# D21/116958
Reviewed / Amended	DATE: <APPROVAL DATE>, REF#: <TRIM REF>
Next Review Date	DATE: <REVIEW DATE>,

CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Legislation / local law requirements	Regulation 17 of the *Local Government (Audit) Regulations 1996.*
Relevant delegations	Nil.
Related policies, procedures and supporting documentation	Risk Management Policy – establishes the risk management responsibilities of Council and Administration and determines quotative and qualitative assessment criteria. Risk Management Procedure – defines the systems and processes of the City's Risk Governance.

INTRODUCTION

Risk appetite refers to the amount and type of risk that the City is willing to accept or retain in order to achieve its objectives. Risk tolerance, on the other hand, is the specific threshold or level of risk that the City considers acceptable.

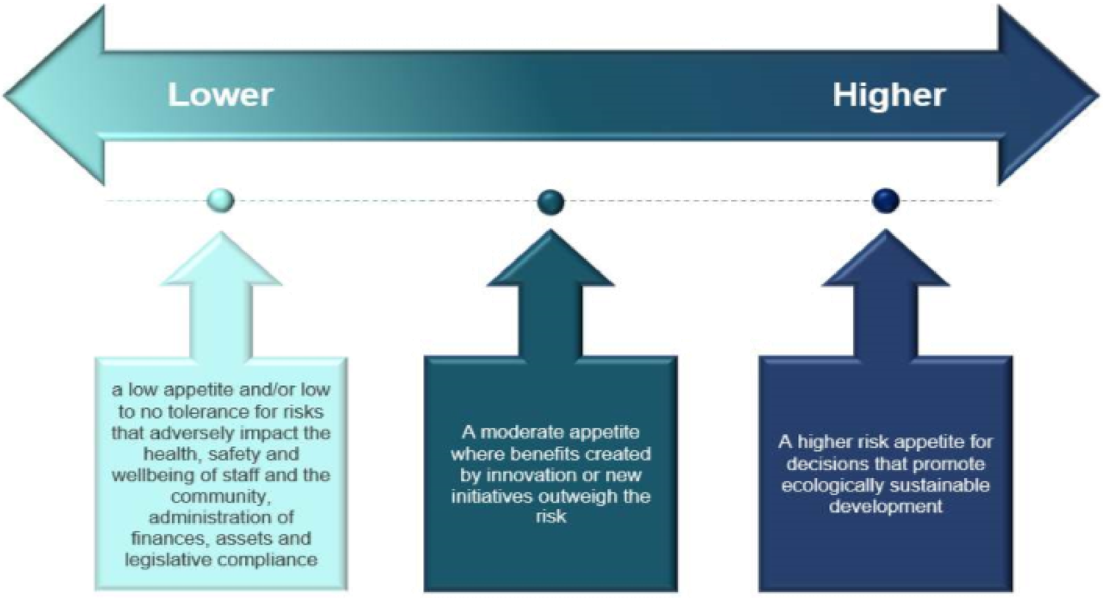
The following statements set boundaries for decision making, ensuring a balance between risk-taking and risk avoidance, and establishes the quantitative and qualitative criteria that determines, classifies, and manages the City's risks.

STATEMENT

The community want us to be a Council and an organisation that is clever, creative, and courageous willing to push the operational boundaries and willing to think and act as an enabler.

We put this into practice in our everyday work and decision making by understanding and managing the risks in being clever and creative but still taking action to meet our strategic goals.

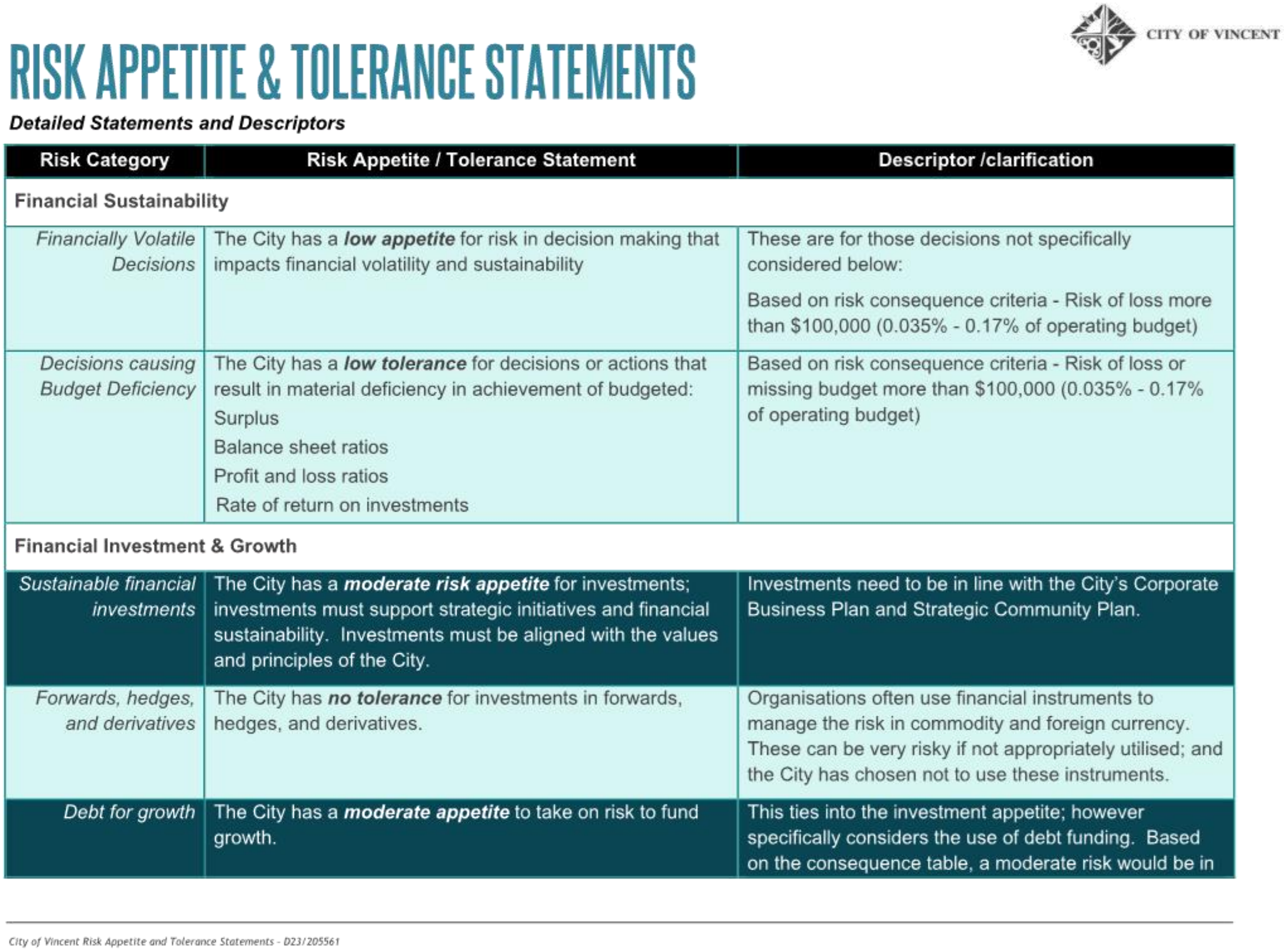
The City seeks to minimise its exposure to key risks relating to people, financial operational and regulatory and compliance responsibilities, while still taking action. We will ensure appropriate measures to mitigate our risks are in place.



a low appetite and/or low to no tolerance for risks that adversely impact the health, safety and wellbeing of staff and the community, administration of finances, assets and legislative compliance

A moderate appetite where benefits created by innovation or new initiatives outweigh the risk

A higher risk appetite for decisions that promote ecologically sustainable development

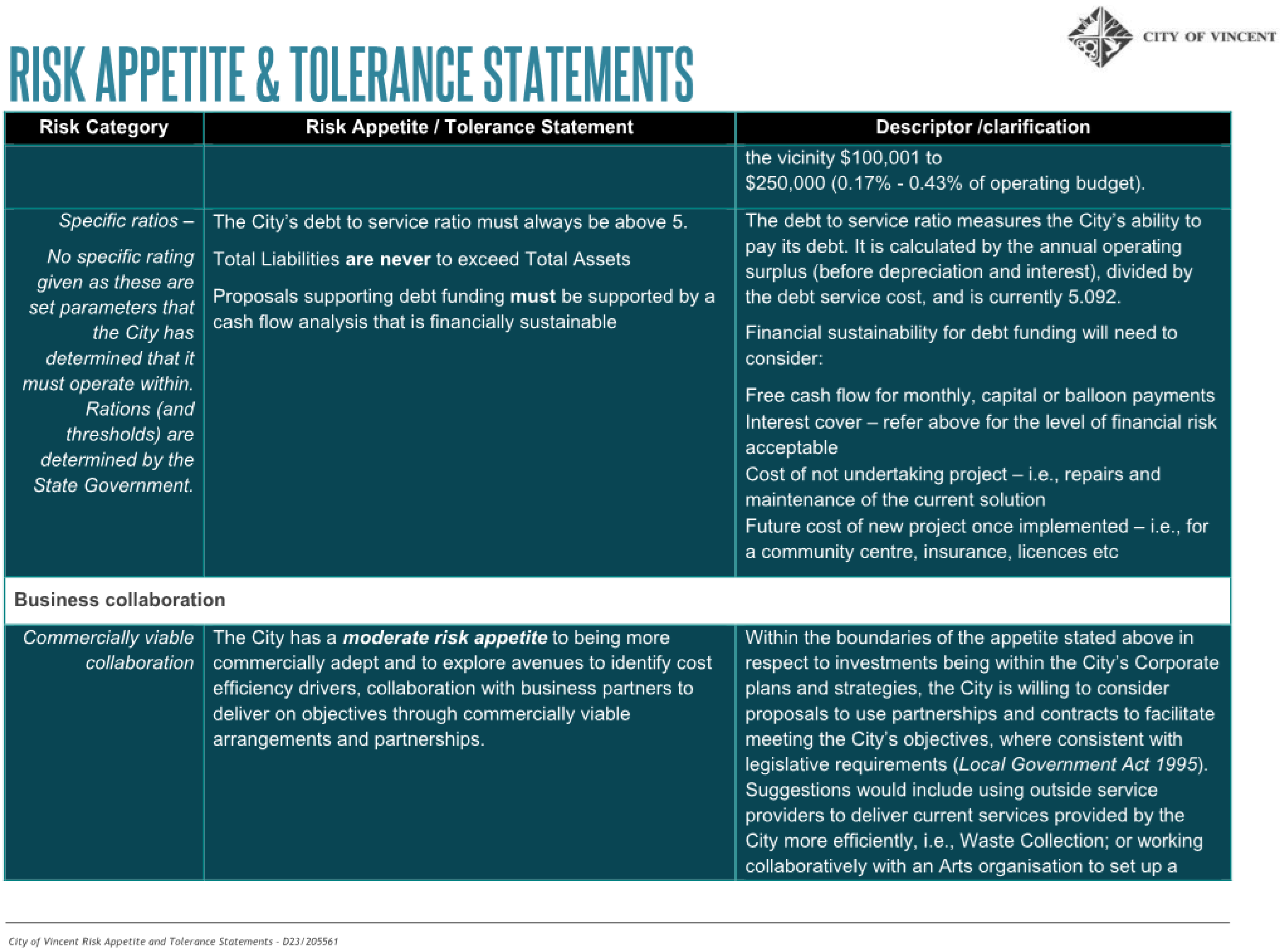


CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Detailed Statements and Descriptors

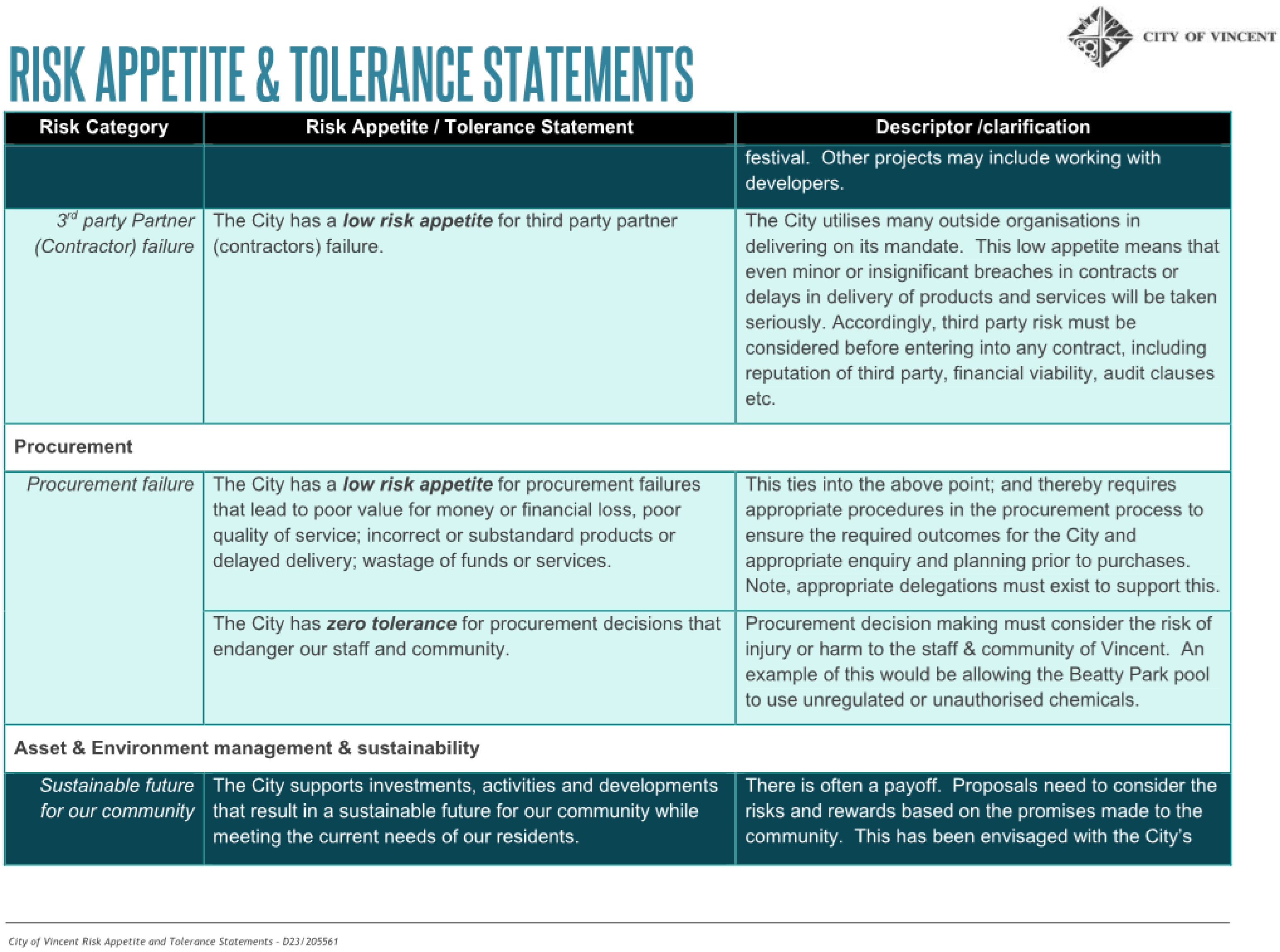
Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
Financial Sustainability		
Financially Volatile Decisions	The City has a ***low appetite*** for risk in decision making that impacts financial volatility and sustainability	These are for those decisions not specifically considered below: Based on risk consequence criteria - Risk of loss more than $100,000 (0.035% - 0.17% of operating budget)
Decisions causing Budget Deficiency	The City has a ***low tolerance*** for decisions or actions that result in material deficiency in achievement of budgeted: Surplus Balance sheet ratios Profit and loss ratios Rate of return on investments	Based on risk consequence criteria - Risk of loss or missing budget more than $100,000 (0.035% - 0.17% of operating budget)
Financial Investment & Growth		
Sustainable financial investments	The City has a ***moderate risk appetite*** for investments; investments must support strategic initiatives and financial sustainability. Investments must be aligned with the values and principles of the City.	Investments need to be in line with the City's Corporate Business Plan and Strategic Community Plan.
Forwards, hedges, and derivatives	The City has ***no tolerance*** for investments in forwards, hedges, and derivatives.	Organisations often use financial instruments to manage the risk in commodity and foreign currency. These can be very risky if not appropriately utilised; and the City has chosen not to use these instruments.
Debt for growth	The City has a ***moderate appetite*** to take on risk to fund growth.	This ties into the investment appetite; however specifically considers the use of debt funding. Based on the consequence table, a moderate risk would be in



CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
		the vicinity $100,001 to $250,000 (0.17% - 0.43% of operating budget).
Specific ratios – *No specific rating given as these are set parameters that the City has determined that it must operate within. Rations (and thresholds) are determined by the State Government.*	The City's debt to service ratio must always be above 5. Total Liabilities **are never** to exceed Total Assets Proposals supporting debt funding **must** be supported by a cash flow analysis that is financially sustainable	The debt to service ratio measures the City's ability to pay its debt. It is calculated by the annual operating surplus (before depreciation and interest), divided by the debt service cost, and is currently 5.092. Financial sustainability for debt funding will need to consider: Free cash flow for monthly, capital or balloon payments Interest cover – refer above for the level of financial risk acceptable Cost of not undertaking project – i.e., repairs and maintenance of the current solution Future cost of new project once implemented – i.e., for a community centre, insurance, licences etc
Business collaboration		
Commercially viable collaboration	The City has a ***moderate risk appetite*** to being more commercially adept and to explore avenues to identify cost efficiency drivers, collaboration with business partners to deliver on objectives through commercially viable arrangements and partnerships.	Within the boundaries of the appetite stated above in respect to investments being within the City's Corporate plans and strategies, the City is willing to consider proposals to use partnerships and contracts to facilitate meeting the City's objectives, where consistent with legislative requirements (*Local Government Act 1995*). Suggestions would include using outside service providers to deliver current services provided by the City more efficiently, i.e., Waste Collection; or working collaboratively with an Arts organisation to set up a

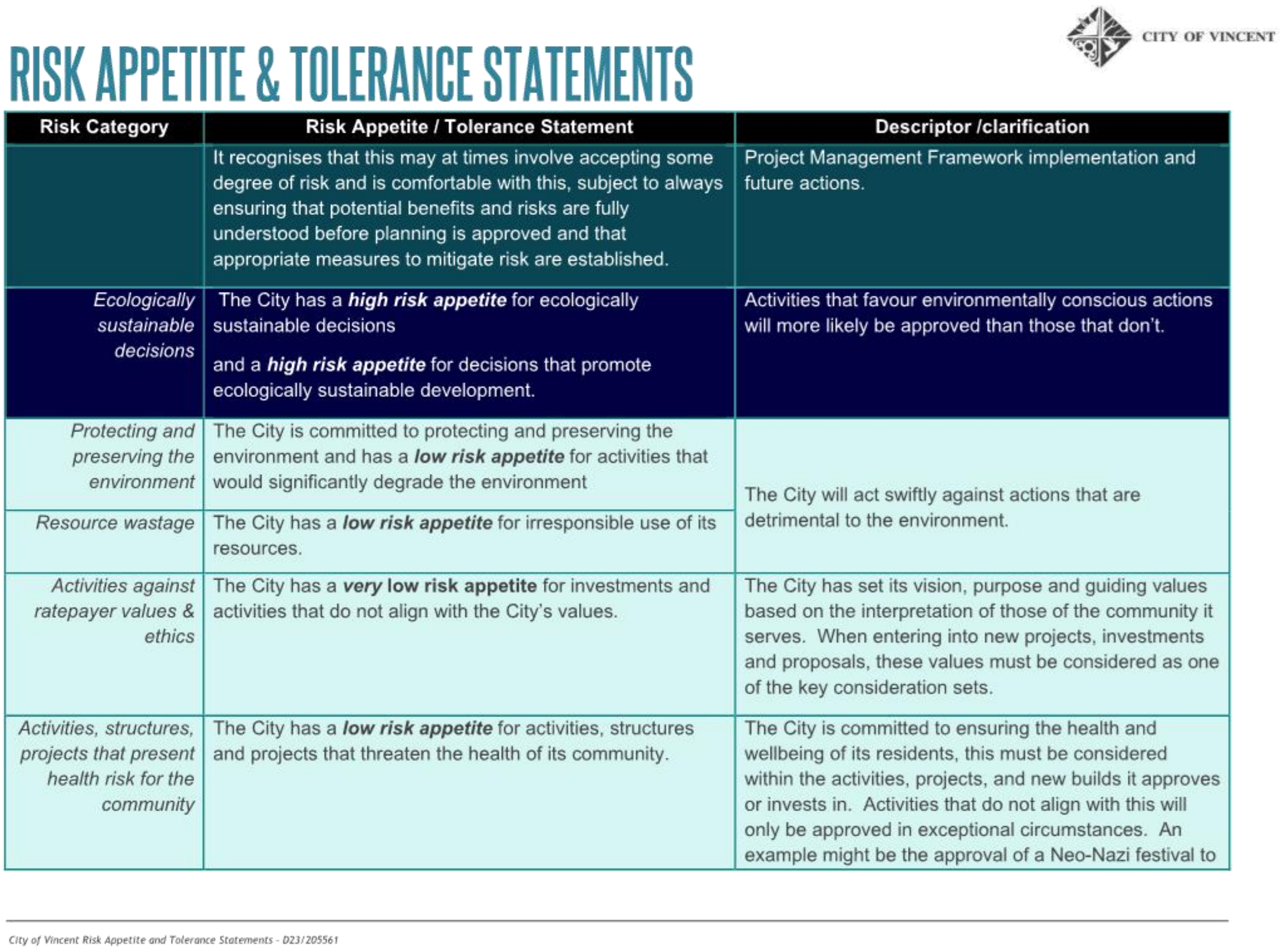


CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
		festival. Other projects may include working with developers.
3rd party Partner (Contractor) failure	The City has a ***low risk appetite*** for third party partner (contractors) failure.	The City utilises many outside organisations in delivering on its mandate. This low appetite means that even minor or insignificant breaches in contracts or delays in delivery of products and services will be taken seriously. Accordingly, third party risk must be considered before entering into any contract, including reputation of third party, financial viability, audit clauses etc.
Procurement		
Procurement failure	The City has a ***low risk appetite*** for procurement failures that lead to poor value for money or financial loss, poor quality of service; incorrect or substandard products or delayed delivery; wastage of funds or services.	This ties into the above point; and thereby requires appropriate procedures in the procurement process to ensure the required outcomes for the City and appropriate enquiry and planning prior to purchases. Note, appropriate delegations must exist to support this.
	The City has ***zero tolerance*** for procurement decisions that endanger our staff and community.	Procurement decision making must consider the risk of injury or harm to the staff & community of Vincent. An example of this would be allowing the Beatty Park pool to use unregulated or unauthorised chemicals.
Asset & Environment management & sustainability		
Sustainable future for our community	The City supports investments, activities and developments that result in a sustainable future for our community while meeting the current needs of our residents.	There is often a payoff. Proposals need to consider the risks and rewards based on the promises made to the community. This has been envisaged with the City's

City of Vincent Risk Appetite and Tolerance Statements - D23/205561



CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
	It recognises that this may at times involve accepting some degree of risk and is comfortable with this, subject to always ensuring that potential benefits and risks are fully understood before planning is approved and that appropriate measures to mitigate risk are established.	Project Management Framework implementation and future actions.
Ecologically sustainable decisions	The City has a ***high risk appetite*** for ecologically sustainable decisions and a ***high risk appetite*** for decisions that promote ecologically sustainable development.	Activities that favour environmentally conscious actions will more likely be approved than those that don't.
Protecting and preserving the environment	The City is committed to protecting and preserving the environment and has a ***low risk appetite*** for activities that would significantly degrade the environment	The City will act swiftly against actions that are detrimental to the environment.
Resource wastage	The City has a ***low risk appetite*** for irresponsible use of its resources.	
Activities against ratepayer values & ethics	The City has a ***very* low risk appetite** for investments and activities that do not align with the City's values.	The City has set its vision, purpose and guiding values based on the interpretation of those of the community it serves. When entering into new projects, investments and proposals, these values must be considered as one of the key consideration sets.
Activities, structures, projects that present health risk for the community	The City has a ***low risk appetite*** for activities, structures and projects that threaten the health of its community.	The City is committed to ensuring the health and wellbeing of its residents, this must be considered within the activities, projects, and new builds it approves or invests in. Activities that do not align with this will only be approved in exceptional circumstances. An example might be the approval of a Neo-Nazi festival to

City of Vincent Risk Appetite and Tolerance Statements - D23/205561

CITY OF VINCENT

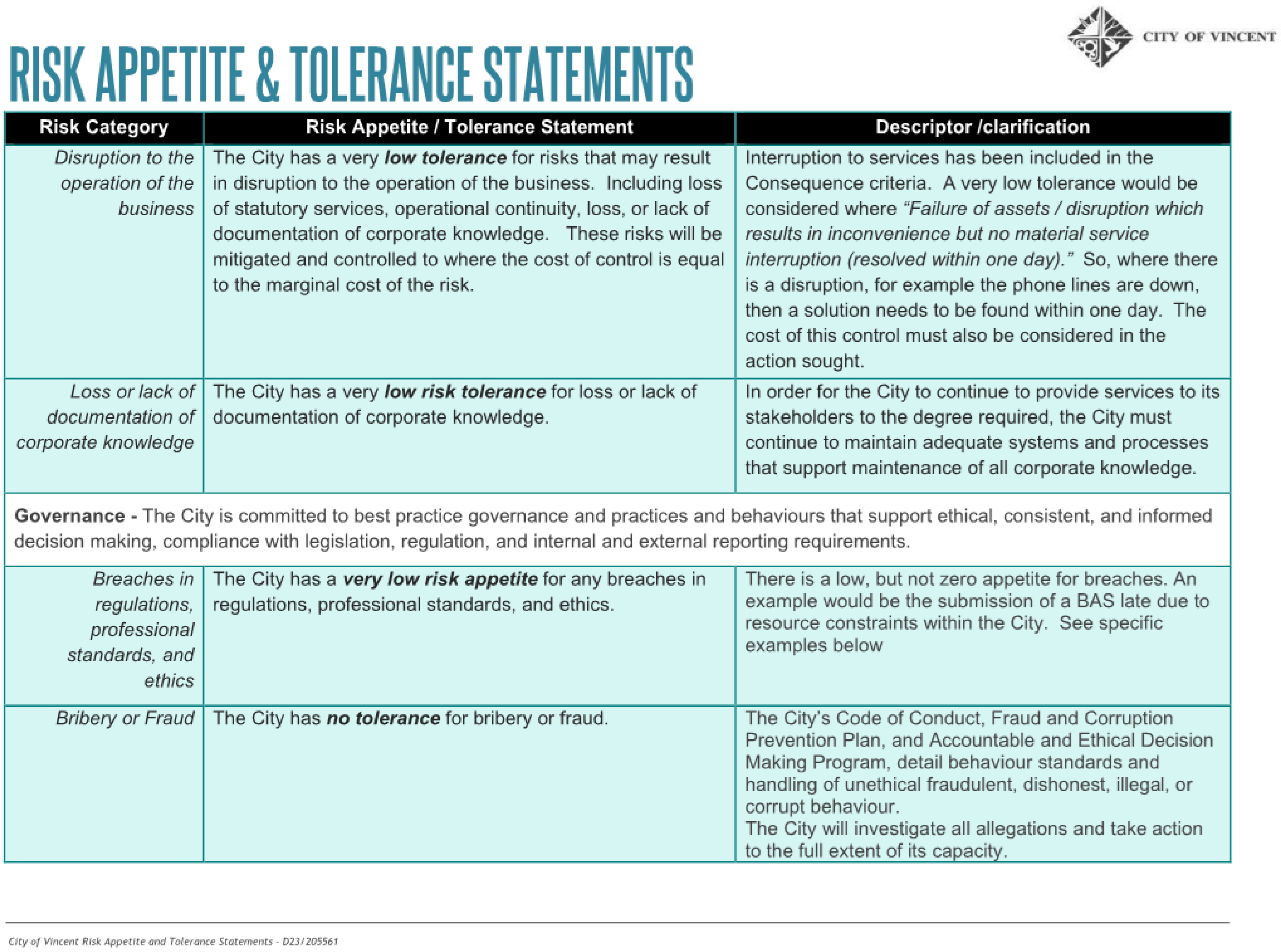
RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
		occur within the City's park space. A multi residential building with no nearby open space may be another example.
Values and Behaviours		
Behaviour or conduct against City values	The City is an equal opportunity employer that employs skilled and experienced employees in positions with clearly defined roles and responsibilities; it has a ***low risk appetite*** for actions and behaviours that threaten the people and organisational capacity.	This sets the City's view on the criticality of its employees and the City culture; accordingly, staff must be selected based on appropriate due diligence and fit for purpose considerations including against the City values. Behaviours and actions of current staff must be measured against their job performance criteria and against the values.
Low individual and team performance	The City places high importance on its values and a culture of integrity in conduct, performance excellence, innovation, equality and diversity, dignity and respect, collegiality, and cultural sensitivity. It has a ***low risk appetite*** for behaviour or conduct which does not meet these standards.	Refer above.
Human Resource		
Behaviour reducing cultural diversity & awareness	The City has a ***low risk appetite*** for practices and behaviours that result in a workforce that is not diverse and culturally aware, be this through recruitment or day to day workplace activities.	Activities and actions to involve and include staff from diverse backgrounds considering culture, age, gender, experience sets etc.
Harm of staff, clients, partners, or visitors	The City has a ***very low risk appetite*** for risk in practices or behaviours that lead to the harm of staff, clients, partners, or visitors in its premises or when undertaking work related activities (within its control and responsibility).	The City's continued focus on OH&S matters, staff and contractor induction support this appetite. All new activities and projects should further consider the impact on the City's community.

CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
Breach of code of conduct, ethics, and Law	The City has ***no appetite*** for conduct that is unlawful, unethical, or otherwise breaches the Code of Conduct or reflects misconduct / serious misconduct.	The City's continued program to educate employees on Code of Conduct, accountability and ethical decision making, performance management and misconduct support this appetite.
Health and Safety		
Inadequate & untimely reporting of breach & near-miss incidents	The City has a ***low appetite*** for health and safety risk, and in particular a ***very low tolerance*** for inadequate or untimely remedy and reporting of breach incidents, or near misses.	The City's continued focus on OH&S matters, staff and contractor induction support this level of appetite and tolerance.
Negligent & deliberate violations of health & safety requirements	The City has ***no tolerance*** for negligent, deliberate, or purposeful violations of health and safety requirements.	
Business Service - The City acknowledges that in order to be innovative and nimble that some degree of risk taking is inevitable, however these risks must be considered in light of maintaining continuity of services to our stakeholders.		

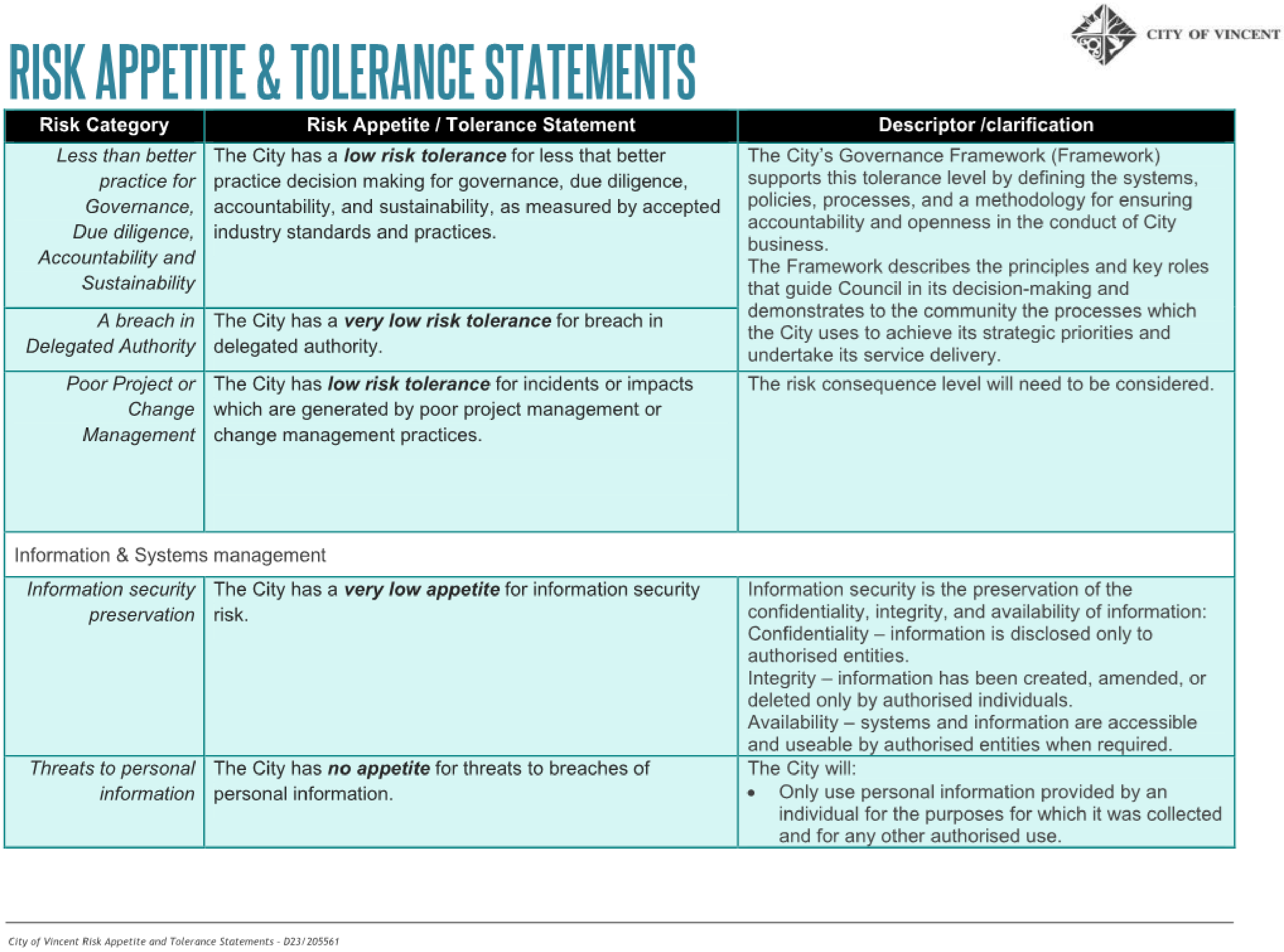


CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
Disruption to the operation of the business	The City has a very ***low tolerance*** for risks that may result in disruption to the operation of the business. Including loss of statutory services, operational continuity, loss, or lack of documentation of corporate knowledge. These risks will be mitigated and controlled to where the cost of control is equal to the marginal cost of the risk.	Interruption to services has been included in the Consequence criteria. A very low tolerance would be considered where *"Failure of assets / disruption which results in inconvenience but no material service interruption (resolved within one day)."* So, where there is a disruption, for example the phone lines are down, then a solution needs to be found within one day. The cost of this control must also be considered in the action sought.
Loss or lack of documentation of corporate knowledge	The City has a very ***low risk tolerance*** for loss or lack of documentation of corporate knowledge.	In order for the City to continue to provide services to its stakeholders to the degree required, the City must continue to maintain adequate systems and processes that support maintenance of all corporate knowledge.
Governance - The City is committed to best practice governance and practices and behaviours that support ethical, consistent, and informed decision making, compliance with legislation, regulation, and internal and external reporting requirements.		
Breaches in regulations, professional standards, and ethics	The City has a ***very low risk appetite*** for any breaches in regulations, professional standards, and ethics.	There is a low, but not zero appetite for breaches. An example would be the submission of a BAS late due to resource constraints within the City. See specific examples below
Bribery or Fraud	The City has ***no tolerance*** for bribery or fraud.	The City's Code of Conduct, Fraud and Corruption Prevention Plan, and Accountable and Ethical Decision Making Program, detail behaviour standards and handling of unethical fraudulent, dishonest, illegal, or corrupt behaviour. The City will investigate all allegations and take action to the full extent of its capacity.

City of Vincent Risk Appetite and Tolerance Statements - D23/205561

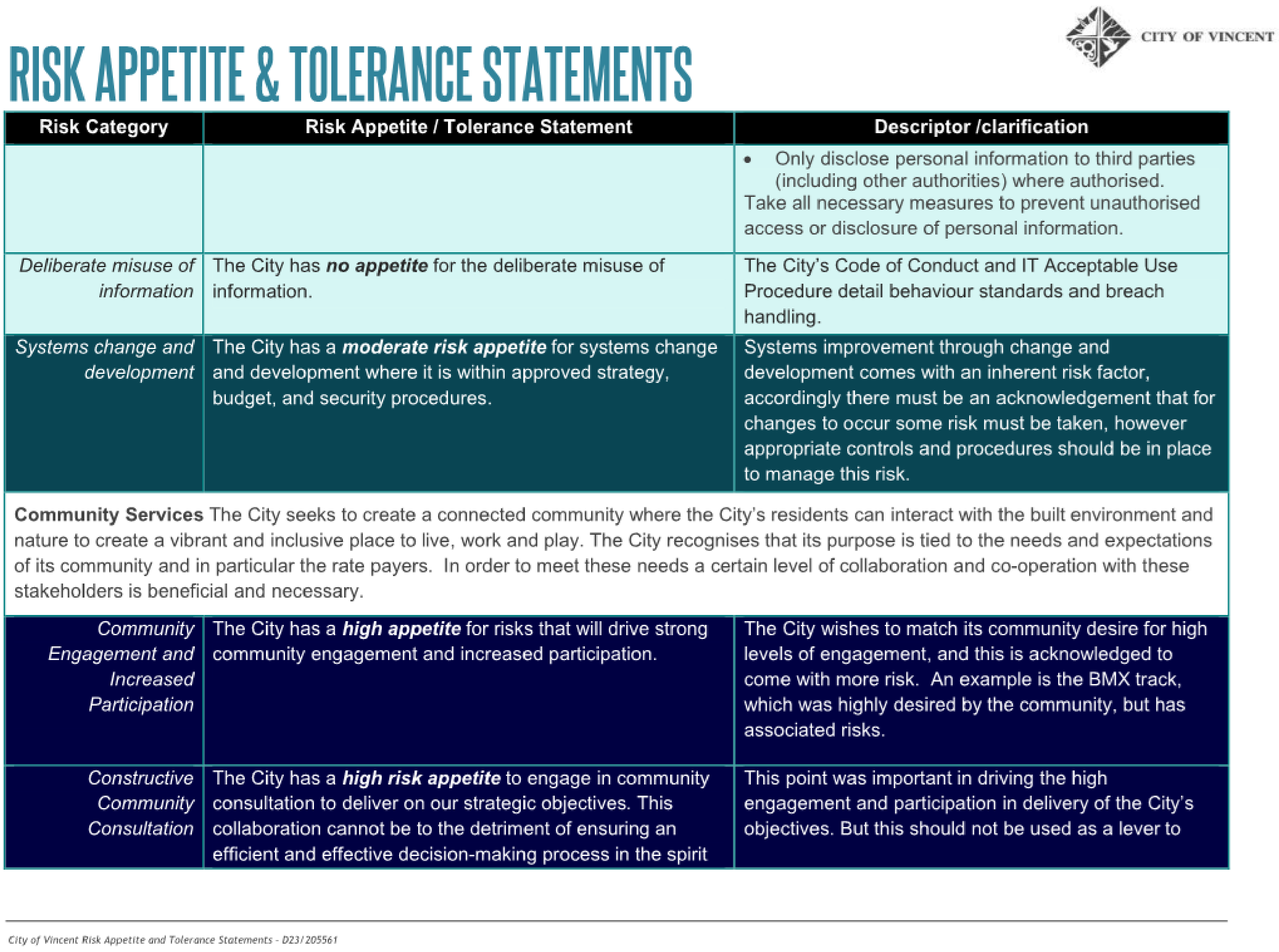


CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
Less than better practice for Governance, Due diligence, Accountability and Sustainability	The City has a ***low risk tolerance*** for less that better practice decision making for governance, due diligence, accountability, and sustainability, as measured by accepted industry standards and practices.	The City's Governance Framework (Framework) supports this tolerance level by defining the systems, policies, processes, and a methodology for ensuring accountability and openness in the conduct of City business. The Framework describes the principles and key roles that guide Council in its decision-making and demonstrates to the community the processes which the City uses to achieve its strategic priorities and undertake its service delivery.
A breach in Delegated Authority	The City has a ***very low risk tolerance*** for breach in delegated authority.	
Poor Project or Change Management	The City has ***low risk tolerance*** for incidents or impacts which are generated by poor project management or change management practices.	The risk consequence level will need to be considered.
Information & Systems management		
Information security preservation	The City has a ***very low appetite*** for information security risk.	Information security is the preservation of the confidentiality, integrity, and availability of information: Confidentiality – information is disclosed only to authorised entities. Integrity – information has been created, amended, or deleted only by authorised individuals. Availability – systems and information are accessible and useable by authorised entities when required.
Threats to personal information	The City has ***no appetite*** for threats to breaches of personal information.	The City will: • Only use personal information provided by an individual for the purposes for which it was collected and for any other authorised use.

City of Vincent Risk Appetite and Tolerance Statements - D23/205561



CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

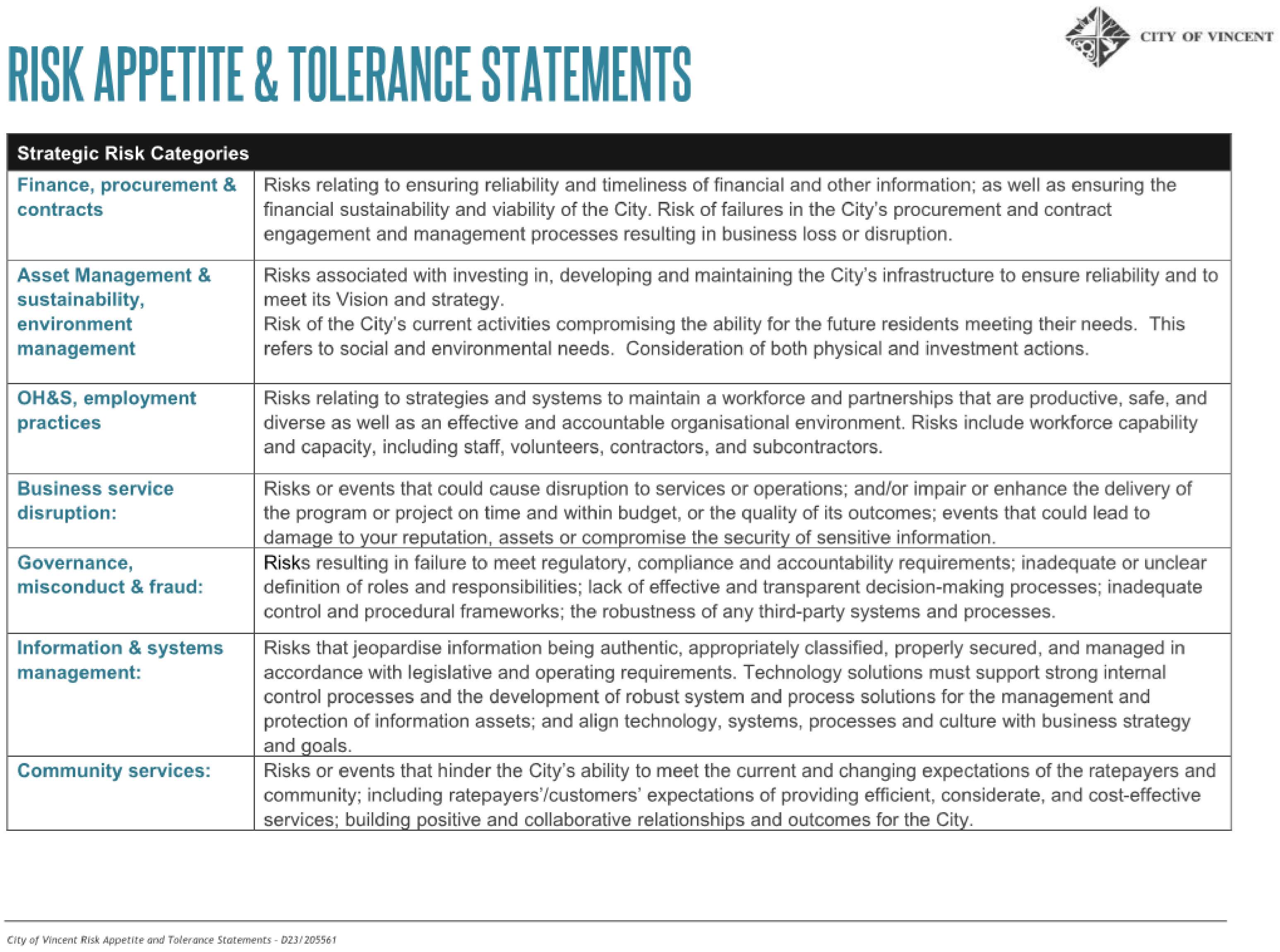
Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
		- Only disclose personal information to third parties (including other authorities) where authorised. Take all necessary measures to prevent unauthorised access or disclosure of personal information.
Deliberate misuse of information	The City has ***no appetite*** for the deliberate misuse of information.	The City's Code of Conduct and IT Acceptable Use Procedure detail behaviour standards and breach handling.
Systems change and development	The City has a ***moderate risk appetite*** for systems change and development where it is within approved strategy, budget, and security procedures.	Systems improvement through change and development comes with an inherent risk factor, accordingly there must be an acknowledgement that for changes to occur some risk must be taken, however appropriate controls and procedures should be in place to manage this risk.
Community Services The City seeks to create a connected community where the City's residents can interact with the built environment and nature to create a vibrant and inclusive place to live, work and play. The City recognises that its purpose is tied to the needs and expectations of its community and in particular the rate payers. In order to meet these needs a certain level of collaboration and co-operation with these stakeholders is beneficial and necessary.		
Community Engagement and Increased Participation	The City has a ***high appetite*** for risks that will drive strong community engagement and increased participation.	The City wishes to match its community desire for high levels of engagement, and this is acknowledged to come with more risk. An example is the BMX track, which was highly desired by the community, but has associated risks.
Constructive Community Consultation	The City has a ***high risk appetite*** to engage in community consultation to deliver on our strategic objectives. This collaboration cannot be to the detriment of ensuring an efficient and effective decision-making process in the spirit	This point was important in driving the high engagement and participation in delivery of the City's objectives. But this should not be used as a lever to

City of Vincent Risk Appetite and Tolerance Statements - D23/205561

CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

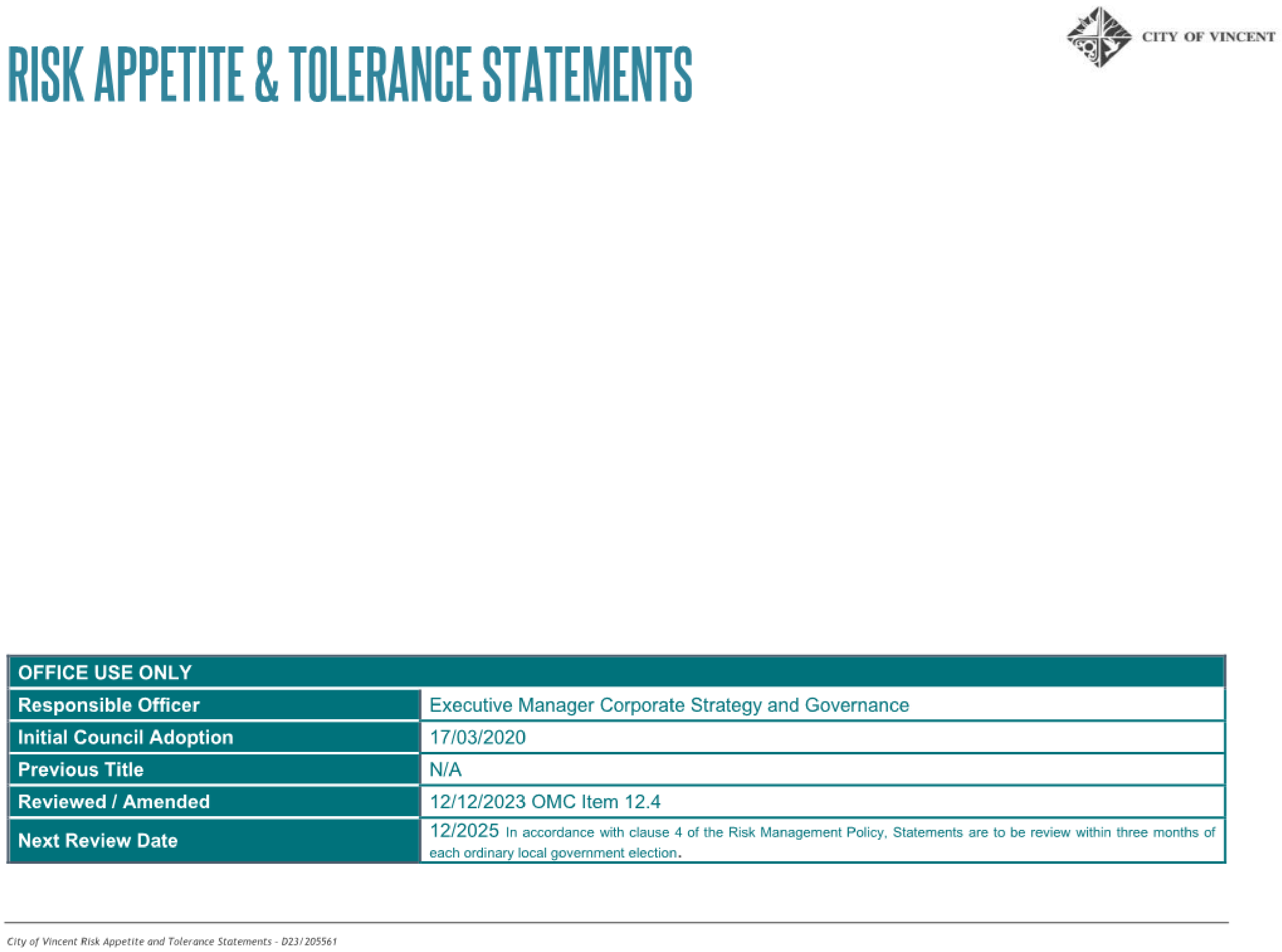
Risk Category	Risk Appetite / Tolerance Statement	Descriptor /clarification
	of sustainability and achievement of objectives. (See sustainability above)	hinder progress or unnecessarily delay decision making.
Activity risking long-term values or reputation of Council	The City has ***zero risk appetite*** in any activity that will put its long-term values or reputation at risk.	
Failure to meet customer commitments and/or provide appropriate advice and address regulatory concerns	The City has a ***very low risk appetite*** for operational risks arising from failure to meet customer commitments and/or appropriateness of advice.	The City must provide appropriate advice to stakeholders and meet its commitments. The City will promptly take action to address ratepayer/customer complaints and regulatory concerns.
Negotiate with Regulators, State & Federal Government Agencies	The City has a ***high risk appetite*** to consult and negotiate with regulators, State & Federal Government Agencies to achieve the City's objectives.	
Leasing of Community Facilities	The City has a ***moderate risk appetite*** for financial loss in respect to the use of the City's community facilities provided the use is: • in the community interest; and • satisfies a recognised community purpose	This is to ensure we are considering the needs of our community together with the financial impacts of decision making.



CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

Strategic Risk Categories	
Finance, procurement & contracts	Risks relating to ensuring reliability and timeliness of financial and other information; as well as ensuring the financial sustainability and viability of the City. Risk of failures in the City's procurement and contract engagement and management processes resulting in business loss or disruption.
Asset Management & sustainability, environment management	Risks associated with investing in, developing and maintaining the City's infrastructure to ensure reliability and to meet its Vision and strategy. Risk of the City's current activities compromising the ability for the future residents meeting their needs. This refers to social and environmental needs. Consideration of both physical and investment actions.
OH&S, employment practices	Risks relating to strategies and systems to maintain a workforce and partnerships that are productive, safe, and diverse as well as an effective and accountable organisational environment. Risks include workforce capability and capacity, including staff, volunteers, contractors, and subcontractors.
Business service disruption:	Risks or events that could cause disruption to services or operations; and/or impair or enhance the delivery of the program or project on time and within budget, or the quality of its outcomes; events that could lead to damage to your reputation, assets or compromise the security of sensitive information.
Governance, misconduct & fraud:	Risks resulting in failure to meet regulatory, compliance and accountability requirements; inadequate or unclear definition of roles and responsibilities; lack of effective and transparent decision-making processes; inadequate control and procedural frameworks; the robustness of any third-party systems and processes.
Information & systems management:	Risks that jeopardise information being authentic, appropriately classified, properly secured, and managed in accordance with legislative and operating requirements. Technology solutions must support strong internal control processes and the development of robust system and process solutions for the management and protection of information assets; and align technology, systems, processes and culture with business strategy and goals.
Community services:	Risks or events that hinder the City's ability to meet the current and changing expectations of the ratepayers and community; including ratepayers'/customers' expectations of providing efficient, considerate, and cost-effective services; building positive and collaborative relationships and outcomes for the City.



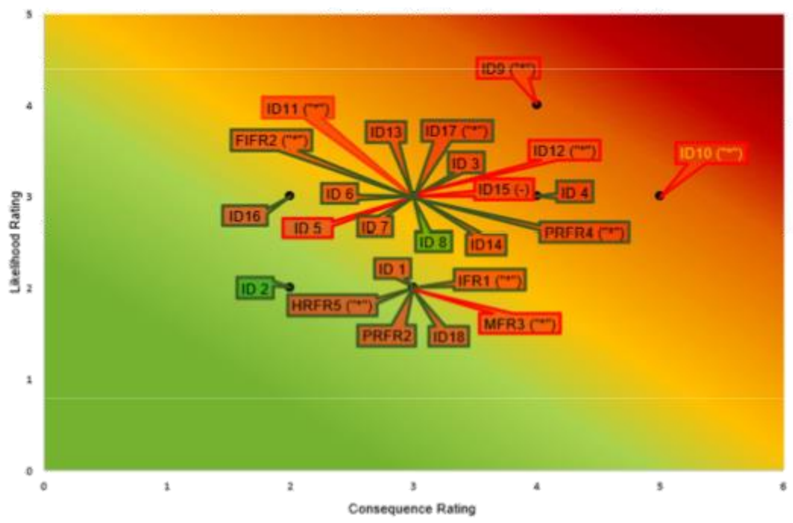
CITY OF VINCENT

RISK APPETITE & TOLERANCE STATEMENTS

OFFICE USE ONLY	
Responsible Officer	Executive Manager Corporate Strategy and Governance
Initial Council Adoption	17/03/2020
Previous Title	N/A
Reviewed / Amended	12/12/2023 OMC Item 12.4
Next Review Date	12/2025 In accordance with clause 4 of the Risk Management Policy, Statements are to be review within three months of each ordinary local government election.

Corporate Risk Rating Alignment to Appetite and Tolerance

Corproate Risk Register - Heat Map - Residual Ratings

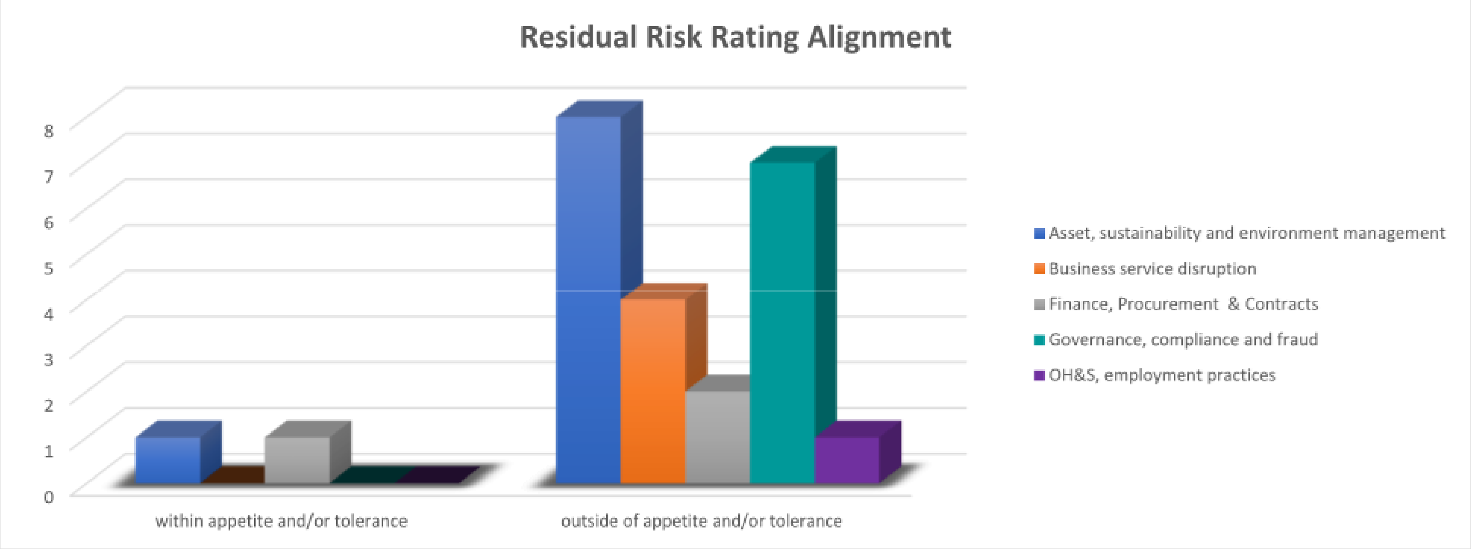


ID Key	Risk Title
ID 1	Supplier / contract management
ID 2	Financial stability, sustainability & reporting
ID 3	Procurement
ID 4	Inadequate asset management
ID 5	Aging / unsafe assets (Leederville Oval grandstand)
ID 6	Aging / unsafe assets (Beatty Park grandstand)
ID 7	Service delivery - 'Industry Education and Enforcement' Health Services
ID 8	Management of Vincent Underground Power Project (VUPP)
~~ID 9~~	~~Polyphagous Shot Hole Borer (PSHB) Management (* March 2024)~~
ID 9	Reduced Urban Tree Canopy Coverage (* December 2024)
ID10	Increased Safety Hazards from Tree Limb Failures (* December 2024)
ID11	Long-term financial impacts of PSHB (* December 2024)
ID12	Reputational Damage due to PSHB (* December 2024)
ID 13	Safety and security practices for staff
ID 14	Disaster Recovery Plan & Business Continuity Management for BPLC
ID 15	Cyber Security
ID 16	Business Continuity through workforce retention
ID 17	Ineffective Business Continuity and Disaster Recovery processes (* March 2024)
ID 18	Corporate governance / legislative compliance
ID FIFR2	Fraudulent Invoicing (* October 2024)
ID HRFR5	Fraudulent deception in recruitment and selection processes (* October 2024)
ID IFR1	Fraudulent disclosure of confidential information (* October 2024)
ID MFR3	Sale of Council Land or Assets (* October 2024)
ID PRFR2	Fraudulent procurement practices (* October 2024)
ID PRFR4	Fraudulent contract management by employee (* October 2024)

Legend				
	🟩	Residual rating within appetite and/or tolerance	" * "	new risk (introduced in the last 12 months)
	🟥	Residual rating outside of appetite and/or tolerance	" - "	risk rating has decreased in last 6 months
	□	Post RMA rating within appetite and/or tolerance	" + "	risk rating has increased in last 6 months
	□	Post RMA rating outside of appetite and/or tolerance		

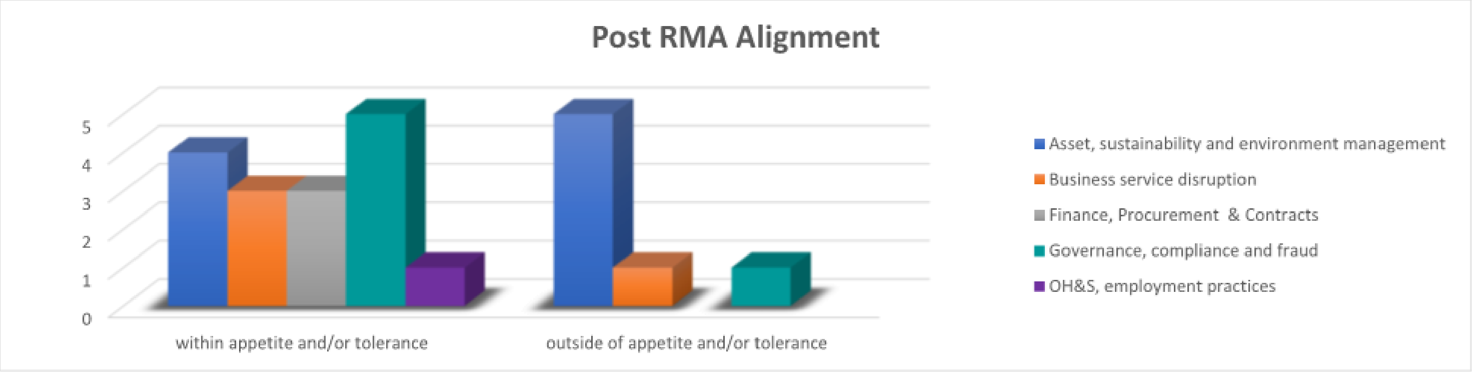
Residual rating alignment is detailed below:

Residual Rating Alignment	Asset, sustainability, and environment management	Business service disruption	Finance, Procurement & Contracts	Governance, compliance, and fraud	OH&S, employment practices	Grand Total
within appetite and/or tolerance	1	0	1	0	0	2
outside of appetite and/or tolerance	8	4	2	7	1	22
	9	**4**	**3**	**7**	**1**	**24**



Post RMA alignment is detailed below:

Post RMA Alignment	**Asset, sustainability, and environment management**	**Business service disruption**	**Finance, Procurement & Contracts**	**Governance, compliance, and fraud**	**OH&S, employment practices**	**Grand Total**
within appetite and/or tolerance	1	0	1	0	0	2
outside of appetite and/or tolerance	8	4	2	7	1	22
	9	**4**	**3**	**7**	**1**	**24**



5.7 AUDIT COMMITTEE - FORWARD AGENDA 2025

Attachments: 1. Audit Committee Forward Agenda 2025 ⇩

RECOMMENDATION:

That the Audit and Risk Committee recommends to Council that it NOTES the Audit and Risk Committee Forward Agenda at Attachment 1.

COMMITTEE DECISION ITEM 5.7

Moved: Mr Manifis, Seconded: Mayor Xamon

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

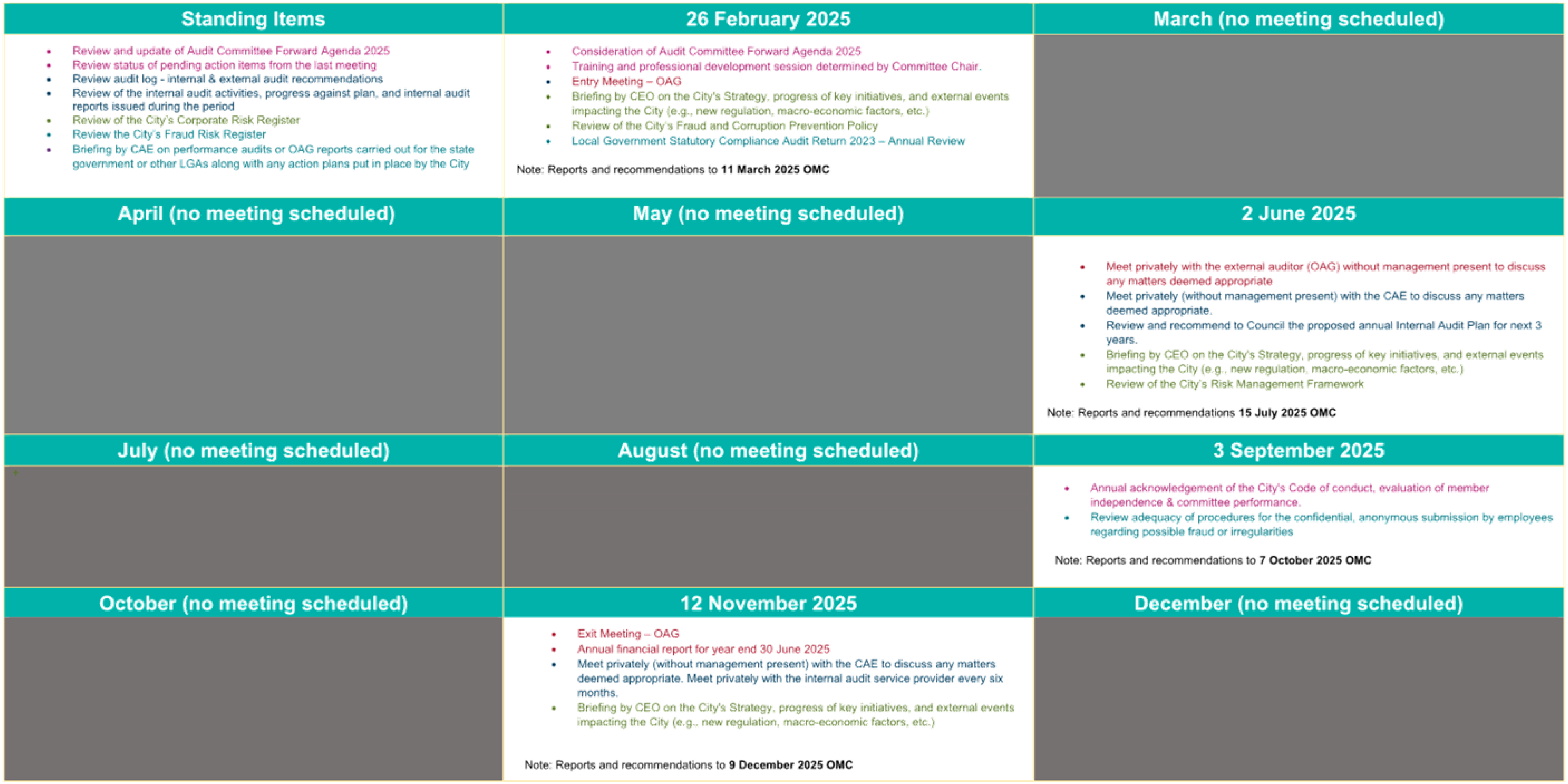
(Cr Alexander was an apology for the Meeting.)

NOTE: The Audit & Risk Committee requested Administration to adjust the forward agenda to:

- Update the 2 June 2025 meeting date to read 2 July 2025
- List the review of the public sector annual submission on integrity and conduct in July.
- Remove the City's Fraud and Corruption Risk Register as a standing item and schedule it for review in September.
- Move the private meeting with the external auditor to November.

.

Audit Committee Forward Agenda 2025



Standing Items	26 February 2025	March (no meeting scheduled)
• Review and update of Audit Committee Forward Agenda 2025 • Review status of pending action items from the last meeting • Review audit log - internal & external audit recommendations • Review of the internal audit activities, progress against plan, and internal audit reports issued during the period • Review of the City's Corporate Risk Register • Review the City's Fraud Risk Register • Briefing by CAE on performance audits or OAG reports carried out for the state government or other LGAs along with any action plans put in place by the City	• Consideration of Audit Committee Forward Agenda 2025 • Training and professional development session determined by Committee Chair. • Entry Meeting – OAG • Briefing by CEO on the City's Strategy, progress of key initiatives, and external events impacting the City (e.g., new regulation, macro-economic factors, etc.) • Review of the City's Fraud and Corruption Prevention Policy • Local Government Statutory Compliance Audit Return 2023 – Annual Review Note: Reports and recommendations to **11 March 2025 OMC**	
April (no meeting scheduled)	**May (no meeting scheduled)**	**2 June 2025**
		• Meet privately with the external auditor (OAG) without management present to discuss any matters deemed appropriate • Meet privately (without management present) with the CAE to discuss any matters deemed appropriate. • Review and recommend to Council the proposed annual Internal Audit Plan for next 3 years. • Briefing by CEO on the City's Strategy, progress of key initiatives, and external events impacting the City (e.g., new regulation, macro-economic factors, etc.) • Review of the City's Risk Management Framework Note: Reports and recommendations **15 July 2025 OMC**
July (no meeting scheduled)	**August (no meeting scheduled)**	**3 September 2025**
		• Annual acknowledgement of the City's Code of conduct, evaluation of member independence & committee performance. • Review adequacy of procedures for the confidential, anonymous submission by employees regarding possible fraud or irregularities Note: Reports and recommendations to **7 October 2025 OMC**
October (no meeting scheduled)	**12 November 2025**	**December (no meeting scheduled)**
	• Exit Meeting – OAG • Annual financial report for year end 30 June 2025 • Meet privately (without management present) with the CAE to discuss any matters deemed appropriate. Meet privately with the internal audit service provider every six months. • Briefing by CEO on the City's Strategy, progress of key initiatives, and external events impacting the City (e.g., new regulation, macro-economic factors, etc.) Note: Reports and recommendations to **9 December 2025 OMC**	

CATEGORIES:

1. **Committee Operations**
2. **Financial Reporting & External Audit (OAG)**
3. **Internal Audit Activities**
4. **Risk Management & Internal Control**
5. **Ethics and Compliance**
6. **Other Matters**

D23/2825

5.8 REVIEW OF THE CITY'S AUDIT LOG

Attachments: 1. Audit Log - Confidential

RECOMMENDATION:

That the Audit Committee recommends to Council that it:

1. NOTES the status of the City's Audit Log at Attachment 1;

2. APPROVES closure of action items noted within this report and at Attachment 1.

COMMITTEE DECISION ITEM 5.8

Moved: Mr Isambert, Seconded: Cr Hallett

That the recommendation be adopted.

CARRIED (6-0)

For: Mr Araj, Mr Manifis, Mr Isambert, Cr Castle, Cr Hallett and Mayor Xamon

Against: Nil

(Cr Alexander was an apology for the Meeting.)

6 GENERAL BUSINESS

6.2 BRIEFING BY CEO - CITY'S STRATEGY, PROGRESS OF KEY INITIATIVES, AND EXTERNAL EVENTS IMPACTING THE CITY

The Chief Executive Officer provided an overview of the City's corporate business plan, highlighting key focus areas, strategic projects, and the importance of the underground power program and tree canopy revitalisation.

6.3 AUDIT & RISK COMMITTEE - SELF-ASSESSMENT SURVEY

The Presiding Member reminded Committee members to complete the Audit & Risk Committee Self-Assessment Survey and noted that the results will be presented to the Committee for consideration at its meeting on 2 July 2025.

7 NEXT MEETING

Wednesday 2 July 2025

8 CLOSURE

There being no further business the meeting closed at 5.37pm.

These Minutes were confirmed at the 2 July 2025 meeting of the Audit & Risk Committee as a true and accurate record of the Audit Committee meeting held on 26 February 2025

Signed: Mr George Araj

Dated