Shire of Dardanup

APPENDICES

ITEM 10

AUDIT & RISK COMMITTEE MEETING

To Be Held

Wednesday, 10th June 2026
Commencing at 3.30pm

At

Shire of Dardanup
ADMINISTRATION CENTRE EATON
1 Council Drive - EATON

This document is available in alternative formats such as:
~ Large Print
~ Electronic Format [disk or emailed]
Upon request.

RISK ASSESSMENT TOOL

REPORT TITLE: *Notification of Counterfeit $20 Note Received*

RISK THEME PROFILE:

8 - Errors, Omissions and Delays

RISK ASSESSMENT CONTEXT: Operational

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	Staff Safety and Customer Interaction. Counterfeit detection often occurs during a face-to-face transaction. Risks include: • potential conflict or aggression from the customer • staff feeling unsure or unsafe in refusing tender	Minor (2)	Unlikely (2)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	Even though the amount is small, accepting a counterfeit note results in a direct financial loss to the Shire. It also establishes a precedent about how such losses are managed across service areas.	Insignificant (1)	Likely (4)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	If counterfeit currency is mishandled (e.g., returned to customer, not reported to police, or evidence contaminated), the Shire may be:	Minor (2)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
	• non-compliant with obligations relating to the *Crimes (Currency) Act* • exposed in an audit (internal or OAG) for poor cash-handling controls • at risk of inconsistent application of procedures across facilities							
REPUTATIONAL	Small failures in financial controls can undermine confidence in: • the Shire's cash-handling processes • staff competency • community trust in the Shire's financial management	Minor (2)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 10.2A)

RISK ASSESSMENT TOOL

REPORT TITLE: Western Australian Auditor General – Schedule of Reports

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Not considering the risks, controls and recommendations arising from the Auditor General's report could have an impact on Council not meeting its compliance requirements.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 10.2B)

Office of the Auditor General
Serving the Public Interest

Report 9: 2025-26 | 6 March 2026

INFORMATION SYSTEMS AUDIT

Microsoft 365 Security Controls – State Entities

Office of the Auditor General for Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Ben Goodwin
Khubaib Gondal
Mushirah Codabaccus
Reshma Vikas
Liam Coetzer

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.

© 2026 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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: OAG

(Appendix AAR: 10.2B)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Microsoft 365 Security Controls – State Entities

Report 9: 2025-26
6 March 2026

This page is intentionally left blank

(Appendix AAR: 10.2B)

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

MICROSOFT 365 SECURITY CONTROLS – STATE ENTITIES

This report has been prepared for submission to Parliament under the provisions of section 24 and 25 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This report summarises the findings of our audit on how effectively seven State government entities manage and secure their Microsoft 365 applications.

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

Caroline Spencer
Auditor General
6 March 2026

Contents

Auditor General's overview 3

Executive summary 4

Introduction 4

Rationale for undertaking this audit 4

Background 4

Conclusion 6

Findings 7

Governance weaknesses undermine security settings 7

Weak identity and access management leave entities exposed to unauthorised access 9

Ineffective information protection could result in data breaches 10

Gaps in security management and visibility increase cyber risks 10

Threat protection controls are partly effective in mitigating cyber threats 11

Recommendations 14

Response from entities 15

Audit focus and scope 16

Appendix 1: MFA types and their strength 17

Auditor General's overview

This report summarises the findings of our audit on how effectively seven State government entities manage and secure their Microsoft 365 (M365) applications. This work was an in-depth assessment of entities' M365 controls carried out alongside our annual general computer controls audits for the 2024-25 financial year. We have not named entities to reduce their risk of exposure to cyber threats.

M365 is widely used by entities to facilitate identity and access, communication, collaboration and information management to deliver essential public services. The security of M365 is dependent on the strength of the security settings that entities implement.

The audit found weaknesses in governance, identity and access management, information protection, logging and monitoring, and threat protection controls. These weaknesses heighten the risk of cyber incidents, data breaches and operational disruptions.

Effective management of M365 security is critical for protecting sensitive government data and maintaining uninterrupted delivery of essential public services amid evolving cyber security threats. I recognise that the rapid and complex evolution of technology consistently presents new challenges for entities. To effectively counter emerging threats, entities must remain alert and continue strengthening their security posture, aligning with better practices and business objectives. They can leverage the progress already made through the implementation of our General Computer Controls audit recommendations, adoption of the Australian Signals Directorate's (ASD) Essential Eight[1] and WA Government Cyber Security Policy.[2]

Case studies are included throughout this report to provide examples of how M365 weaknesses can impact entities. I encourage all public sector entities to review these case studies and implement the recommendations outlined in this report.

[1] Australian Government, *Essential Eight*, Australian Signals Directorate website, November 2023, accessed 25 February 2026.

[2] Department of the Premier and Cabinet, *WA Government Cyber Security Policy*, WA.gov.au website, October 2025, accessed 25 February 2026.

Executive summary

Introduction

This audit assessed seven State government entities' effectiveness in managing and configuring their M365 applications and security controls to minimise the risk of cyber incidents, data breaches and service disruptions.

The audit focused on security controls applied to the M365 environment and applications that support collaboration and data sharing (Figure 1). It did not include end-user applications such as Microsoft Word, Excel, PowerPoint and Outlook.

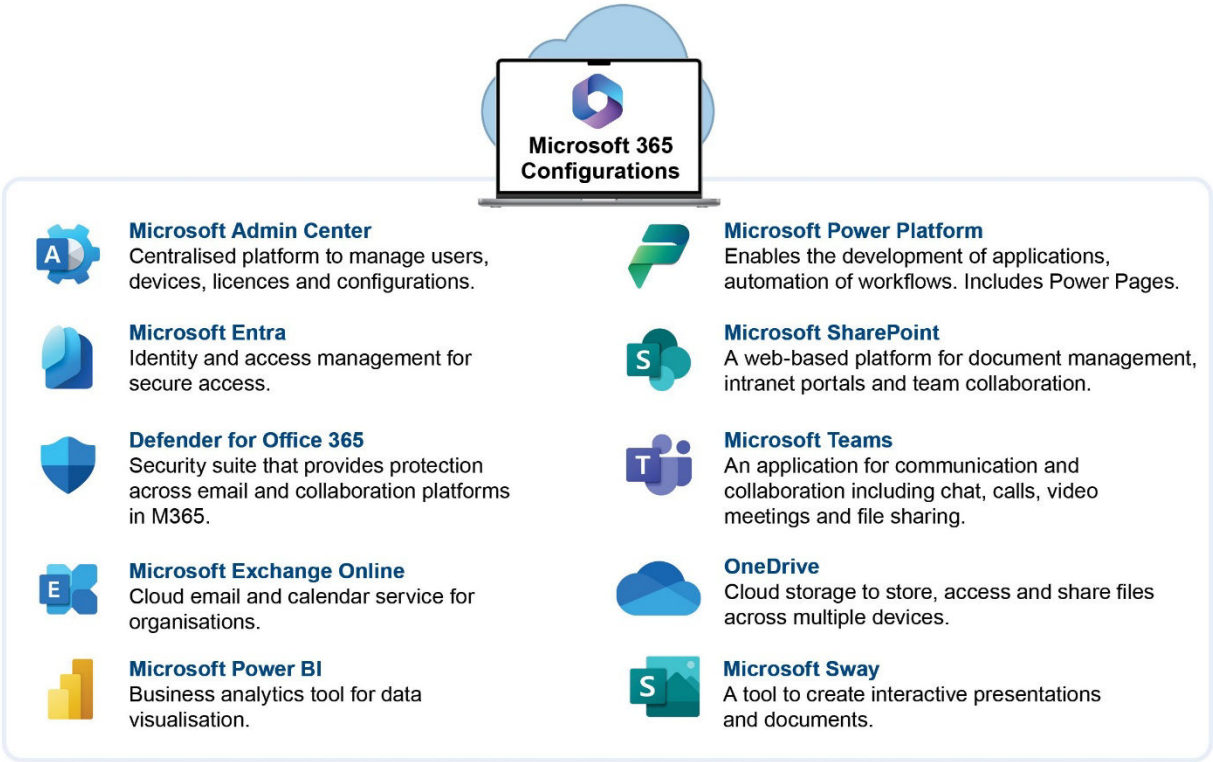
We provided detailed findings and recommendations to all entities during the audit. This report summarises our audit findings. Entities are not named to minimise the risk of compromise.

Rationale for undertaking this audit

Cyber security threats are evolving and can seriously disrupt important services delivered by entities. With the increasing reliance on M365 for identity and access, collaboration, data storage and sharing, it is essential entities appropriately manage and configure M365 security settings to prevent cyber incidents, data breaches and service disruptions. The audit aimed to identify common security gaps and opportunities for improving entities' M365 security.

Background

M365 is a suite of productivity and collaboration applications used by most entities to help deliver services to the Western Australian public. It includes a comprehensive set of configurations (security settings) to safeguard applications and the information they hold.



Source: OAG

Figure 1: Microsoft 365 areas covered in the audit

The protection of an M365 environment is only as strong as the security settings applied by an entity. Misconfigured settings, overly permissive access or a lack of security and controls monitoring can result in threat actors[3] gaining unauthorised access to entity systems and information.

The pace of technological change poses ongoing challenges for entities. Entities must remain alert to new security threats and continuously review their M365 security settings in line with better practices. This includes guidance provided by:

- Center for Internet Security
- Cybersecurity and Infrastructure Security Agency, United States Government - this is also recommended by the Office of Digital Government[4]
- Australian Signals Directorate
- Microsoft.

At each audited entity, we assessed the effectiveness of more than 160 M365 security settings based on better practice standards. We grouped these into five categories (Figure 2).

Source: OAG

Figure 2: Security setting categories covered by our audit

[3] Any individual or group (e.g. nation-state actors, cyber criminals or insiders) that intentionally cause harm to systems, network or data. Examples of harm include theft of information, service disruptions, system compromise and misuse of access.

[4] Department of the Premier and Cabinet - Office of Digital Government Security Operations Centre, *Secure Cloud Business Applications*, WA Cyber Security Unit (DGov Technical) website, January 2024, accessed 6 January 2026.

Conclusion

Entities are only partly effective in managing and configuring their M365 applications and security settings and need to do more to minimise the risk of cyber incidents, data breaches and service disruptions.

Most audited entities had established cyber security policies and implemented foundational M365 security settings, but these offered only limited protection and were rarely aligned to industry better practice.

We identified significant and moderately rated weaknesses across four of the five security setting categories: governance; identity and access management; information protection; and security management and visibility. While entities had implemented a range of controls in the threat protection category, minor weaknesses were identified across all entities rendering the controls only partly effective.

Collectively, the weaknesses we identified undermine the overall security of entities' M365 environments and increase the likelihood of data breaches, disrupted operations and cyber incidents.

Findings

Table 1 shows the rating of weaknesses for each entity's security settings across the five audited categories.

Audited category	Entities						
	1	2	3	4	5	6	7
Governance	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Identity and access management	Moderate	Moderate	Moderate	Moderate	Moderate	Significant	Moderate
Information protection	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Significant
Security management and visibility	Minor	Minor	Moderate	Moderate	Moderate	Moderate	Moderate
Threat protection	Minor	Minor	Minor	Minor	Minor	Minor	Minor

Significant Moderate Minor

Source: OAG

Table 1: Effectiveness of audited entities' security settings by category

Governance weaknesses undermine security settings

Entities had documented policies and procedures to oversee information and cyber security risks and practices. However, they did not cover M365 security settings which were not effectively implemented and rarely aligned to industry best practice. This means entities were left vulnerable to cyber incidents, data breaches and operational disruptions.

Five entities had all of the following weaknesses. The remaining two had three of the below:

- **Minimum security requirements were not defined –** entities did not use a better practice standard to set minimum M365 security requirements, despite a recommendation from the Office of Digital Government[5] to do so. Important settings may not have been implemented, exposing entities to data loss, operational disruption and reputational damage. Entities also did not monitor for unauthorised changes to, or deviations from, M365 security settings to detect vulnerabilities and misconfigurations.
- **Security settings were not backed up –** entities did not backup M365 configurations including security policies, access controls and application settings. Entities lack the ability to quickly restore security and operational settings following accidental changes, malicious alterations or failures.

[5] The Department of the Premier and Cabinet - Office of Digital Government Security Operations Centre, *Secure Cloud Business Applications*, WA Cyber Security Unit (DGov Technical) website, January 2024, accessed 6 January 2026.

- **Personal devices were allowed but not managed –** entities allowed staff to use personal devices (e.g. personal computers, mobiles) to register[6] multifactor authentication (MFA) and access M365 applications without these devices being enrolled in the entities' device management systems. Personal devices should be enrolled in a device management system to reduce the risk of a threat actor using stolen credentials and then registering their own device for MFA. This also secures access to work related applications and data, and provides entities with a mechanism to remotely wipe government data without affecting personal content. The high-profile 2022 Medibank data breach[7] occurred through an exploited personal device.
- **Not all users and access rights were reviewed –** entities have implemented user account reviews but they did not cover all types of M365 accounts such as cloud only users, service accounts[8] or external guest users. In addition, although entities appropriately approved access by third-party applications to their M365 environment, they did not periodically review this access to determine if it was still required.
- **There was a lack of assurance over cloud security –** entities were not reviewing cloud security or assurance reports[9] to understand their security posture[10] and known gaps in controls or risks that may require their attention. This lack of oversight can leave entities vulnerable to data breaches and unable to manage risks before they escalate.

Case study 1: Inconsistent implementation of security settings weakens overall security

An entity we audited shared a M365 environment with another entity.[11] While the audited entity had generally good practices, the second had applied inconsistent security settings which weakened the overall security of the shared environment. This occurred despite the entities having a security committee which oversees and coordinates configuration changes for the shared environment.

Examples of security settings that did not align between the two entities include:

- The audited entity had blocked legacy authentication[12], the other did not.
- Automated responses to high-risk user activity were implemented by the first entity, but not the second.

An attacker could compromise the M365 environment by exploiting weak settings at the second entity. The compromise would impact both entities due to the shared environment.

[6] A process to setup the device (e.g. phone) and methods (e.g. authenticator app) for multifactor authentication.

[7] Office of the Australian Information Commissioner, *Medibank data breach: alleged timeline*, OAIC website, n.d., accessed 30 October 2025.

[8] A service account is a non-human login that lets systems and applications work automatically in the background.

[9] Cloud vendors generally provide annual independent assurance reports that must be considered. Examples of these reports include system and organisation controls type 2 reports on security controls and their effectiveness, and the InfoSec Registered Assessors Program assessment against the Australian Information Security Manual requirements.

[10] How protected and prepared an entity is against cyber threats.

[11] This second entity was not part of our audit scope.

[12] Legacy authentication protocols cannot enforce MFA. These include Active Sync, Autodiscover, POP3, IMAP and SMTP.

Weak identity and access management leave entities exposed to unauthorised access

Entities were not effectively minimising the risk of unauthorised access. Weak identity and access management controls, including the use of insecure authentication methods, leave entities vulnerable to compromise. Compromised accounts were responsible for 39% of reported cyber incidents targeting the Australian Government[13] in 2024-25. Many of the identified weaknesses are relatively easy and inexpensive to fix.

Three entities had all of the following weaknesses. The remaining four had three of the below:

- **MFA controls could be strengthened –** entities have not implemented phishing-resistant MFA (Appendix 1), particularly for accounts with higher privileges. They used SMS, voice and email one-time passwords which are highly susceptible to phishing attacks and contributed to the highest number (58%) of security incidents affecting the Australian Government in 2024-25.[14]

  The Australian Cyber Security Centre reported that threat actors are exploiting weaker MFA methods for data theft, extortion and other criminal activities.[15] These attacks combine technical skills and social engineering to compromise one-time password MFA authentication. Where entities don't enforce the use of managed devices to perform MFA, threat actors may configure devices outside the entities' control to gain persistent access.

- **Legacy authentication methods were used –** entities did not block legacy authentication methods. These old and vulnerable methods could be used to bypass MFA and are more susceptible to credential theft and brute-force[16] attacks.

- **Privileged identity management (PIM) was not appropriate –** entities had PIM but staff were still being granted permanent access to privileged roles rather than only for the time needed to perform a specific task. This practice undermines the effectiveness of PIM in minimising the overall attack surface[17] and exposure to potential threats.

- **Cloud accounts were generally not used for privileged access –** entities use on-premise active directory[18] accounts, rather than cloud based privileged accounts, to manage their M365 environments. On-premise accounts do not include the enhanced security features available in M365. It is better practice to separate on-premise and cloud management accounts to reduce the spread of potential breaches.

---

[13] Australian Signals Directorate, *Annual Cyber Threat Report 2024-2025*, Australian Cyber Security Centre website, 14 October 2025, accessed 15 October 2025.

[14] Ibid.

[15] Australian Signals Directorate, *Joint advisory released on recent activity by Scattered Spider threat actors | Cyber.gov.au*, Australian Cyber Security Centre website, 30 July 2025, accessed 6 November 2025.

[16] A method threat actors use to try and guess passwords by trying every possible combination until they find the right one.

[17] An attack surface is all the different points on the network that an attacker could try to compromise. This can include websites, applications, user accounts, connected devices, third-party vendors and physical access points.

[18] Active directory manages entity users, computers and access rights.

Ineffective information protection could result in data breaches

Entities had broad and unrestricted external sharing permissions which undermine their ability to monitor information flow and enforce policies. This makes it harder to detect and respond to inadvertent or intentional data breaches.

All entities had the following weaknesses:

- **Data loss prevention (DLP) controls were not broadly implemented –** entities had DLP policies but they were not applied to OneDrive, SharePoint, Power Platform, Exchange and Teams. Additionally, where policies were implemented, they did not protect all sensitive data types.
- **Poor data sharing controls –** entities did not appropriately restrict the sharing of information through SharePoint, Sway, Power Platform, Teams and OneDrive. Administrator approval was also not required for any staff to create public facing Power Page websites. Poor data sharing controls increase the likelihood of unintentional data sharing with external parties.
- **Data storage was not restricted to approved locations –** staff could save documents to unapproved third-party locations (e.g. Dropbox, Facebook, Google Drive, OneDrive Personal) and synchronise data from their work OneDrive to unmanaged devices. Entities cannot appropriately protect and restrict access to government information stored in locations outside of their device management system.

Case study 2: Third-party data breach

An audited entity emailed personal and sensitive information about 32 individuals (including minors) to a third-party service provider, who then stored it in Dropbox. A cyber security incident later exposed this information to an unknown threat actor.

The entity did not have DLP controls to protect the information and confirm the extent of exposure. The entity also did not perform a security assessment of the third-party during vendor onboarding.

Gaps in security management and visibility increase cyber risks

All entities were using a security information and event management system to log and monitor M365 security events. However, gaps in logging and monitoring impede entities' ability to respond to security incidents and collectively lessen protection against insider and external threats.

Three entities had all of the following weaknesses. The remaining four had three or more of the below:

- **Privileged roles were not adequately monitored –** the allocation or change of highly privileged roles did not always generate alerts. This means significant changes to access rights were not promptly brought to the attention of relevant entity staff. Malicious or accidental privilege escalation can occur without detection, increasing the likelihood of data breaches, misconfigurations or unauthorised actions.

- **Security management features were not appropriately controlled –** any user could create a new M365 tenant[19] and become its highly privileged administrator. Without visibility it will be difficult for entities to oversee the new tenancy and enforce security policies in these tenants to reduce the occurrence of accidental or intentional misconfigurations that might lead to data breaches.

  Additionally, not all administrator portals were restricted to privileged users. Disclosure of configuration details may heighten the risk of privilege escalation if a standard user account is compromised.

- **Vendor access was not effectively controlled –** only one entity used M365's built-in vendor access process (Customer Lockbox), which gives entities better control and visibility over vendor staff access. The Customer Lockbox adds an extra layer of protection and oversight as the process requires formal authorisation before any vendor access to entity data is granted.

- **Logs were not retained for long enough –** entities had enabled some M365 security logs and were monitoring security events. These logs were being retained for between six months and 10 years. Additional logs could be enabled to improve visibility (for example, risky user actions) and should be retained long enough to trace the origin and full impact of security incidents (such as when someone accessed or modified sensitive information and what was accessed or modified). The ASD recommends logs be kept for at least 18 months.[20]

- **Guest access needs to be strengthened –** any user could invite guests[21] to access sensitive data, often without needing administrator approval. Additionally, entities allowed staff to invite guests from anywhere, instead of limiting guests to trusted entities. Consequently, users may permit external access that elevates the likelihood of accidental or intentional data leakage.

Threat protection controls are partly effective in mitigating cyber threats

Entities have implemented a range of threat protection controls. They generally scanned and blocked harmful files transmitted through emails or shared on OneDrive, SharePoint and Teams. Common executable files[22] were also prevented to reduce the risk of harmful software. However, minor weaknesses remain that erode the overall security posture of entities.

All entities had the following weaknesses:

- **High-risk users and sign-ins were not always blocked –** entities did not consistently block high-risk and suspicious sign-ins, such as those trying to access sensitive resources or sign in from unusual locations or unknown devices. Additionally, entities did not receive a notification to trigger a review when such sign-ins were detected. Unusual activity may not be investigated in a timely manner.

[19] An M365 tenant is a dedicated private space for an entity in the cloud. It is where all entity services reside such as Teams, OneDrive and SharePoint.

[20] Australian Signals Directorate, *Strategies to mitigate cybersecurity incidents: Mitigation details*, Australian Cyber Security Centre website, 1 February 2017, accessed 16 December 2025.

[21] An individual from outside the entity who is invited to access and collaborate.

[22] Executable files run programs or applications and are often used by attackers to introduce malware.

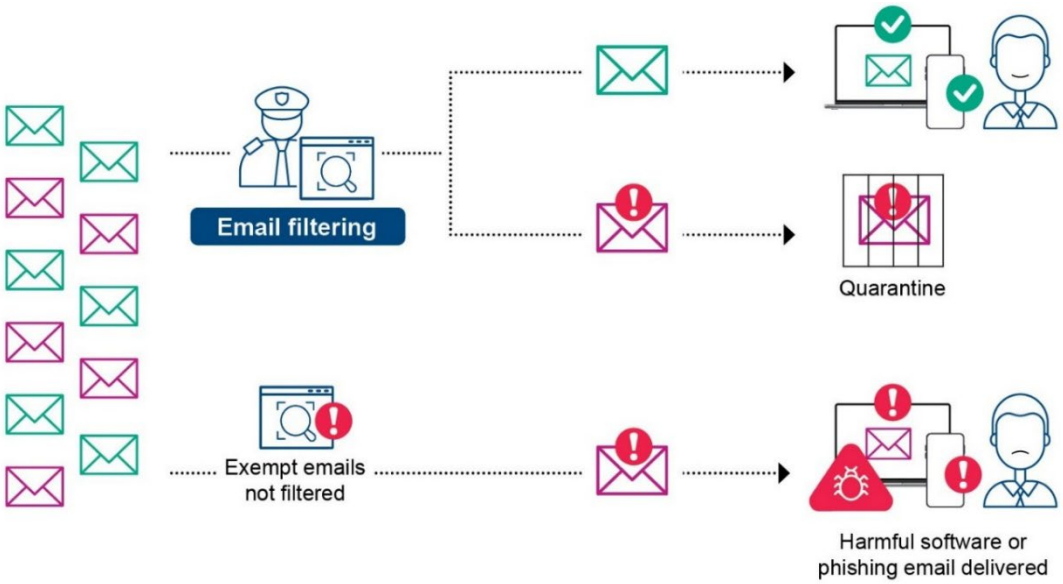
A number of entities did enforce MFA authentication when a high-risk sign-in was detected.

- **Customised security settings did not always provide protection –** instead of using M365 preset security settings, which provide centrally managed, consistent and balanced protection against phishing, spam and malware, entities applied their own customised security settings. These did not always provide the same level of control and protection.

- **Email protections were not fully effective –** entities did not apply appropriate controls to prevent the impersonation of sensitive users and partner domains[23], for example through email spoofing. They also did not implement effective controls[24] that would allow third party email servers to identify and report fake or suspicious emails claiming to be from the entities. This increases the likelihood of successful impersonation, data breaches and financial loss.

  In addition, entities did not prevent the email platform from automatically forwarding emails to external recipients. This is often exploited in business email compromise scams to automatically send emails, including sensitive or confidential information, to external parties without oversight or approval. The Australian Federal Police reported more than $152 million was stolen in business email compromise scams in 2024[25]. One of the tactics reported include automatic email forwarding.

  Furthermore, while entities had email filtering to reduce the likelihood of malicious emails reaching staff, they exempted certain organisations or email platforms instead of individual people. This leaves staff more susceptible to receiving spam and phishing emails which can result in credential compromise or the inadvertent downloading of harmful software (Figure 3). It is better practice to limit exemptions in M365 to trusted individuals instead of entire organisations.



Source: OAG

Figure 3: Lack of email filtering can lead to compromise

[23] Partner domains are other organisations that entities collaborate with.

[24] Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication, Reporting and Conformance provide a mechanism for email servers to automatically identify, block and report fraudulent emails to the entity being impersonated. This requires email servers to have these controls.

[25] Australian Federal Police, Criminals target construction sector with Business Email Compromise scams, AFP website, 28 October 2025, accessed 12 November 2025.

- **Malicious code could be introduced –** entities did not restrict staff from installing unapproved Teams applications or block external code being used in Power BI. Unvetted applications can contain vulnerabilities or malicious code that provide threat actors with an avenue to exploit the application and access an entity's sensitive information. Most entities did not enforce content security policies for Power Platform, increasing their susceptibility to web-based code attacks such as cross-site scripting.[26] These types of attacks can allow threat actors to manipulate content and steal entity information.

Case study 3: Business email compromise results in financial loss

An M365 account and weak MFA belonging to an entity's[27] senior officer was compromised by a threat actor using a targeted phishing email. This breach remained undetected for a month, during which time the entity ignored multiple suspicious activity warnings and the threat actor:

- registered their own MFA methods using an unmanaged overseas device
- created email forwarding rules to hide email communication from the account holder
- studied the officer's email history to construct a believable scenario, before emailing fraudulent invoices and approving their payment.

The threat actor used this access to steal $71,000 from the entity. The entity recovered the money through insurance and its bank but has not yet fixed the underlying weak M365 controls.

The entity was also not able to carry out a full investigation as it did not maintain sufficient logs.

[26] Cross-site scripting is a type of attack where malicious code is injected into a trusted website. As a result, sensitive user data like login credentials, session tokens or session cookies may be stolen leading to a full account compromise. These attacks can also redirect users of a legitimate website to fake sites spreading harmful software.

[27] We identified this issue during our 2025 annual general computer controls audit. The entity was not part of the M365 audit.

Recommendations

1. To strengthen cyber security governance, the entities should:
    a. use better practice standards to develop and implement minimum M365 security requirements balancing risk and business needs
    b. use the Department of the Premier and Cabinet's (Office of Digital Government) tools and resources to enhance M365 security[28]
    c. ensure M365 services can be restored from backup, redeployed through automation or rebuilt from documentation, to meet organisational requirements and security baselines
    d. monitor configurations for deviations against the baseline
    e. use device management systems to register unmanaged personal devices
    f. regularly seek assurance over cloud security controls.
2. To enhance system identity and access management, the entities should:
    a. use phishing resistant MFA for privileged users
    b. transition non-privileged accounts using weak MFA to stronger authentication methods with better phishing resistance (Appendix 1)
    c. migrate legacy access accounts to modern authentication methods and block legacy authentication
    d. use privileged access management systems to ensure just-in-time access controls
    e. use cloud only accounts to manage M365 environments.
3. To protect information, the entities should:
    a. implement data loss prevention controls over M365 applications and data
    b. restrict data storage to approved locations and services
    c. use data sharing controls to limit sharing with only authorised parties.
4. To improve information and cyber security management and visibility of threats, the entities should:
    a. continuously monitor all high-risk security events including assignment and use of privileges
    b. use M365 built-in vendor access processes
    c. retain logs for adequate periods
    d. control guest access.
5. To enhance threat protection, the entities should:
    a. block high-risk users and sign-ins until reviewed
    b. enforce M365 preset security settings for improved protection against phishing, spam and malware, or implement an equivalent level of custom defined controls
    c. implement impersonation protection controls including for partner domains

[28] The Department of the Premier and Cabinet, Office of Digital Government Security Operations Centre, Secure Configuration Assessment Guideline, WA Cyber Security Unit (DGov Technical) website, November 2024, accessed 17 February 2026.

d. implement controls to check the authenticity of emails
e. limit the use of exemptions and filter emails to prevent phishing and malicious software
f. apply content security policies to prevent common web-based threats
g. limit users from installing unapproved applications.

Response from entities

All audited entities generally agreed with detailed findings and recommendations.

Audit focus and scope

The audit objective was to assess the effectiveness of seven State government entities in managing and configuring their M365 Cloud applications and security controls to minimise the risk of cyber incidents, data breaches and service disruptions.

In undertaking the audit, we reviewed better practice guidance including:

- Center for Internet Security – Microsoft 365 Foundation Benchmark[29]
- Cybersecurity and Infrastructure Security Agency, United States Government – Microsoft 365 Secure Configuration Baseline (the controls specific to the US government were adapted for an Australian context)
- Australian Signals Directorate – Blueprint for Secure Cloud[30]
- Microsoft better practice guides.[31]

The audit aimed to identify common security gaps and opportunities for improving the entities' M365 security. This work was carried out alongside our annual general computer controls audits for the 2024-25 financial year and was considerably more in-depth, involving a comprehensive assessment of the management and configuration of Microsoft 365 applications and security controls within seven State government entities.

We ran automated tools[32] and, where required, performed manual procedures to verify the effectiveness of entities' controls. If entities used third-party services and software alongside M365 controls, we also evaluated these to determine the overall effectiveness of their security measures.

This was an independent audit conducted under the *Auditor General Act 2006* and arising from our information systems functions. We complied with the independence and other ethical requirements related to assurance engagements. The approximate cost of undertaking the audit and reporting was $195,000.

[29] Center for Internet Security, *CIS Microsoft 365 Benchmarks*, CIS website, n.d., accessed 26 February 2025.

[30] Australian Signals Directorate, *Configuration | ASD's Blueprint for Secure Cloud*, ASD website, n.d., accessed 20 February 2025.

[31] Microsoft Ignite, *Advanced deployment guides for Microsoft 365* , MS Website, 10 March 2025, accessed 27 March 2025.

[32] Cybersecurity & Infrastructure Security Agency, *Assess the state of M365*, GitHub website, n.d., accessed 26 February 2025.

Appendix 1: MFA types and their strength

MFA type		Description	Phishing resistance	Primary threats
	SMS-based one-time password (OTP)	A one-time password is received via SMS	Weak	SIM swapping, phishing/smishing, malware, call/SMS interception, social engineering
	Voice-based OTP	A one-time password is received via phone call	Weak	
	Email-based OTP	A one-time password is received via email	Weak	Phishing/smishing, malware, email interception, social engineering
	App-based time-limited OTP	A mobile app generates a time-based one-time password (TOTP)	Weak	Malware, social engineering, lost/damaged phone, compromised app backups (e.g. via Microsoft account compromise)
	Authenticator App push with context	The authenticator app prompts the user to approve/deny login. It may require number matching and can provide requesting application's name and the user's location.	Better	Social engineering, lost/damaged phone, notification fatigue. These risks are somewhat reduced by providing context information and requiring number matching.
	Biometric (face/fingerprint)	Uses biometric features to authenticate and may be passwordless	Best	Physical injury
	Hardware security key (FIDO2)[33]	A physical hardware security key is used to authenticate, and may be passwordless	Best	Damaged, lost or stolen security key
	Passkeys (FIDO2)	Passkeys are enrolled and securely stored on a device for use when authenticating	Best	Malware, damaged/lost/stolen device, compromised cloud sync services

Source: OAG

[33] FIDO2 (Fast Identity Online 2) is an open standard for secure passwordless authentication and MFA.

This page is intentionally left blank

Auditor General's 2025-26 reports

Number	Title	Date tabled
9	Microsoft 365 Security Controls – State Entities	6 March 2026
8	Status of Local Government Audits 2025	28 January 2026
7	State Government 2025 – Information Systems Audit Results	3 December 2025
6	State Government 2025 – Financial Audit Results	3 December 2025
5	Valuation of Property Held by the Public Education Endowment Trust	3 December 2025
4	WA's Progress to Implement the National Principles for Child Safe Organisations (arising from the Royal Commission into Institutional Responses to Child Sexual Abuse)	27 November 2025
3	Maintaining Regional Local Roads	12 November 2025
2	Gold Corporation – Trade Applications	29 October 2025
1	Management of Housing Maintenance Information	6 August 2025

(Appendix AAR: 10.2B)

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

(Appendix AAR: 10.2C)

Office of the Auditor General
Serving the Public Interest

Report 10: 2025-26 | 6 March 2026

PERFORMANCE AUDIT

Controls Over Portable Assets – State Entities

Office of the Auditor General for Western Australia

Audit team:
Aloha Morrissey
Justine Mezzatesta
Claire Lieb
Else Harris
Jenna Fuller
Nathan Johnston

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.

© 2026 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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/Thanapoom+Limchuchua

(Appendix AAR: 10.2C)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Controls Over Portable Assets – State Entities

Report 10: 2025-26
6 March 2026

This page is intentionally left blank

(Appendix AAR: 10.2C)

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

CONTROLS OVER PORTABLE ASSETS – STATE 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 if five State government entities had effective controls over their portable assets to minimise loss and misuse.

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

Caroline Spencer
Auditor General
6 March 2026

Contents

Auditor General's overview 3

Executive summary 4

Introduction 4

Rationale for undertaking the audit 4

Background 4

Conclusion 7

Findings 8

Entities do not have a good understanding of their portable assets 8

Entities' disposal practices need improvement 12

Staff are guided on the personal use of portable assets to prevent misuse 12

Recommendations 14

Response from audited entities 15

Audit focus and scope 16

Auditor General's overview

State government entities use a diverse range of assets in their delivery of services to the community. This audit focussed on portable assets with an individual value of less than $5,000. Portable assets include safety devices, medical and scientific equipment, maintenance and workshop tools, educational aids and information technology equipment. Collectively, these portable assets represent a significant investment of government funds and are at high risk of loss or misuse as they are easily moved and are often attractive for theft for personal use or gain by on-selling.

Entities are required to put in place effective controls across all their assets, including portable assets, to ensure they are available when needed for service delivery, to safeguard them against misuse and loss, and protect employees from accusations of wrongdoing. Each entity is responsible for implementing controls to safeguard assets, balanced with administrative effort, cost and risk. This includes clear policies and procedures to ensure consistency and accountability, particularly when asset management is assigned to operational areas and to staff who work in different locations, including regional and remote sites.

Of the five entities we audited, only ChemCentre had a full understanding of what portable assets they had and where they were located. They also conducted regular stocktakes and had good disposal records. ChemCentre's controls minimised the likelihood of service disruption, misuse and loss. In stark contrast, the Forest Products Commission did not know what portable assets they had and were not conducting stocktakes.

However, I am pleased that all the entities are educating staff about appropriate use of these assets through integrity training programs. I also acknowledge challenges for entities that manage a large and diverse range of portable assets shared across multiple sites.

As part of this audit, we reviewed our own portable asset controls and identified areas for improvement including updating policies and procedures to remove inconsistencies and ensure alignment with upgraded systems and correcting minor inaccuracies within registers.

I thank the staff at each of the audited entities for their cooperation and assistance in completing this work. I strongly encourage all public sector entities to consider the findings in this report and assess their own portable asset controls, policies and practices to ensure taxpayer funds are not wasted through misuse or theft.

Executive summary

Introduction

This audit assessed if the following five State government entities had effective controls over their portable assets to minimise loss and misuse:

- ChemCentre
- Forest Products Commission (FPC)
- Metropolitan Cemeteries Board (MCB)
- North Metropolitan TAFE (NM TAFE)
- WA Country Health Service (WACHS).

We focussed on a sample of their portable assets that are critical to entity operations with an individual value of less than $5,000.

Rationale for undertaking the audit

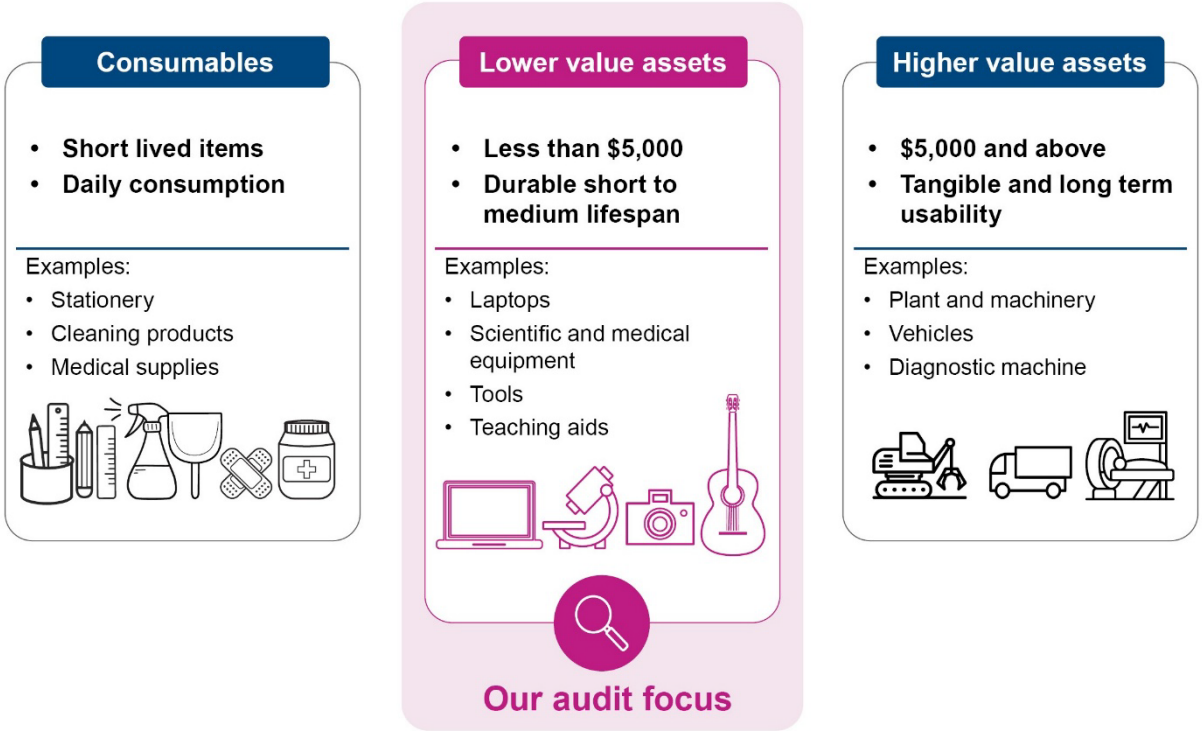
Entities are required to responsibly manage all assets entrusted to them and ensure they are available for delivery of their services. This audit complements our existing financial audit coverage of asset procurement and controls over higher value assets.

We last audited this topic in the State sector in 2017[1] and found registers were inaccurate and incomplete and did not always contain enough information to monitor and track assets properly.

Background

Entities use a variety of assets to deliver services to the community (Figure 1). While lower in value, portable assets represent a high risk of loss and misuse because they are easily moved and are often attractive for personal use. They may also need regular servicing and maintenance to ensure they are safe to use and are functioning well. Entities need to put in place appropriate measures to monitor and track these assets, so they are available for use when needed and to safeguard them against misuse and loss.

[1] Office of the Auditor General, *Financial Controls – Focus Area Audits 2016-17*, OAG website, 7 November 2017, accessed 10 November 2025.



Source: OAG

Figure 1: Types of entity assets and our area of focus

When determining what portable assets to track, entities should consider including portable assets that are:

- critical to operations – those that require ongoing servicing and calibration to be fit-for-use, such as medical devices and scientific equipment (blood pressure monitors, microscopes, digital thermometers and gas detectors)
- important for safety and emergency response – such as GPS and satellite communication devices that support off-site and remote operations
- at risk of data security breaches – those that contain sensitive data and provide access to systems, such as laptops and mobile phones
- at risk of misuse and theft – such as audio-visual equipment (cameras), small appliances (food processors), musical instruments (guitars) and gardening and power tools (drills, chainsaws, and mowers).

Entities determine the types and value of items to include on their asset registers. Figure 2 shows the diverse range of portable assets used by the five entities we assessed. Additionally, these entities also manage other portable assets that we did not review in our audit.

Source: OAG

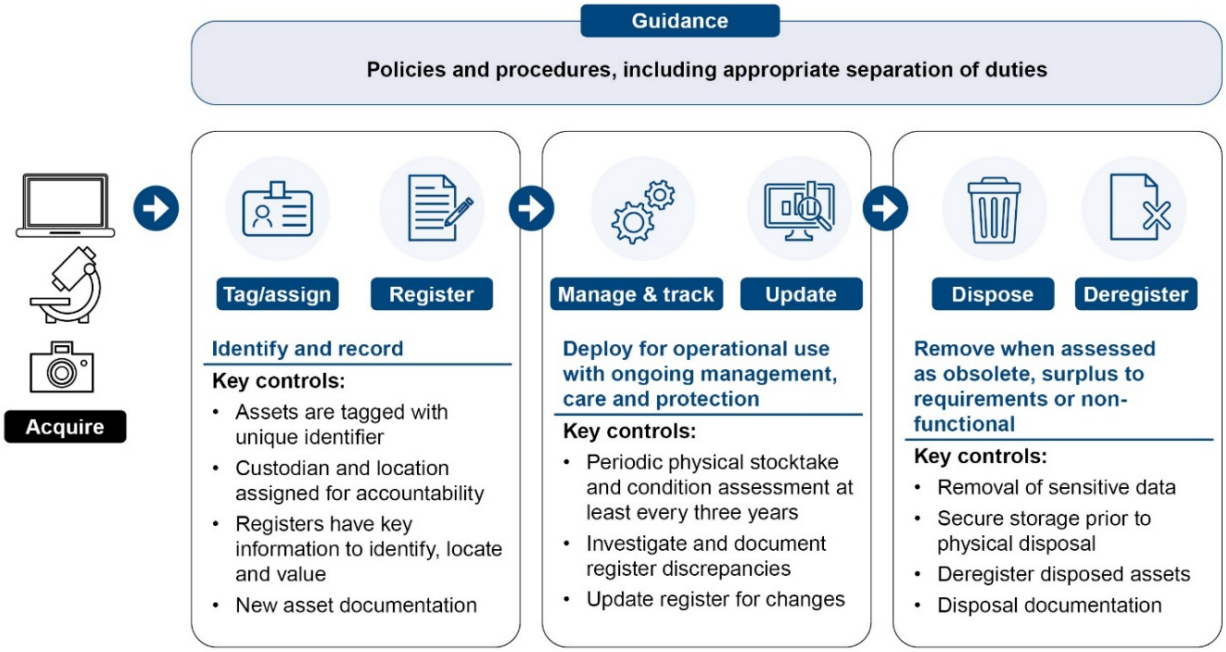
Figure 2: Portable assets included in the registers we assessed

Entities are required to manage and protect public property, including portable assets, and foster a workplace culture of ethical behaviour to minimise the risk of loss, misuse and theft.[2] To meet these requirements, entities should have suitable controls in place, including clear policies and procedures to record the custody, use and disposal of portable assets. Policies should outline appropriate separation of duties to ensure key responsibilities for asset registration, tracking and disposal are completed by different staff positions to reduce the risk of error, misappropriation and loss. These should be clearly and regularly communicated to staff, so they are aware of their roles and responsibilities in managing and safeguarding portable assets, and expectations around appropriate personal use of these assets. This is

[2] In conducting the audit, we considered the requirements of the *Financial Management Act 2006* and associated *Treasurer's Instructions and guidance*, *Public Sector Management Act 1994* and *Public Sector Commissioner's Instructions*, *Procurement Act 2020*, *Western Australian Procurement Rules and guidance*.

particularly important when asset management is devolved to operational areas and to staff who work in different locations.

Figure 3 shows the key controls we assessed during the audit.



Source: OAG

Note: Procurement and acquisition of portable assets was not assessed in this audit. All areas above are considered as part of our annual financial audits. In the areas within scope of this audit, we went much deeper than is necessary or cost-effective in an annual financial audit.

Figure 3: Portable asset key controls

Conclusion

Of the five audited entities, only ChemCentre had effective controls to record, track and dispose of its portable assets. MCB, NM TAFE and WACHS' controls were partly effective, while FPC's were mostly not effective. Weak controls increase the risk that items will be misused, lost or stolen and not be available for service delivery when needed.

More than a third of portable assets at FPC, MCB, NM TAFE and WACHS could not be found due to inaccurate registers and inadequate tracking. Entities did not consistently record new assets or remove lost or disposed of items from their registers. In addition, while stocktakes are a key control to help entities manage their assets, these were not always being regularly or sufficiently performed. Without accurate and complete registers supported by comprehensive stocktakes, entities do not have a good understanding of what assets they have available, their condition and what they might need to buy or replace in the future.

The same four entities also had weaknesses in their disposal policies and practices. This included not having appropriate approvals and not documenting the reason for and method of disposal. These entities need to improve their documentation and disposal practices to ensure unauthorised disposals do not go unnoticed.

All audited entities made staff aware of their responsibilities around the personal use of portable assets through mechanisms such as codes of conduct and refresher training. This helps to create a culture of accountability and reduces the risk of portable asset misuse and financial loss by the State and, ultimately, cost to the taxpayer.

Findings

We assessed the effectiveness of controls for the recording, tracking, disposal and use of portable assets and identified weaknesses and areas for improvement (Table 1).

	ChemCentre	FPC	MCB	NM TAFE	WACHS
Registers are complete and accurate	●	●	●	●	●
Stocktakes are periodically performed	●	●	●	●	●
Disposals are appropriate	●	●	●	●	●
Clear guidance on personal use	●	●	●	●	●

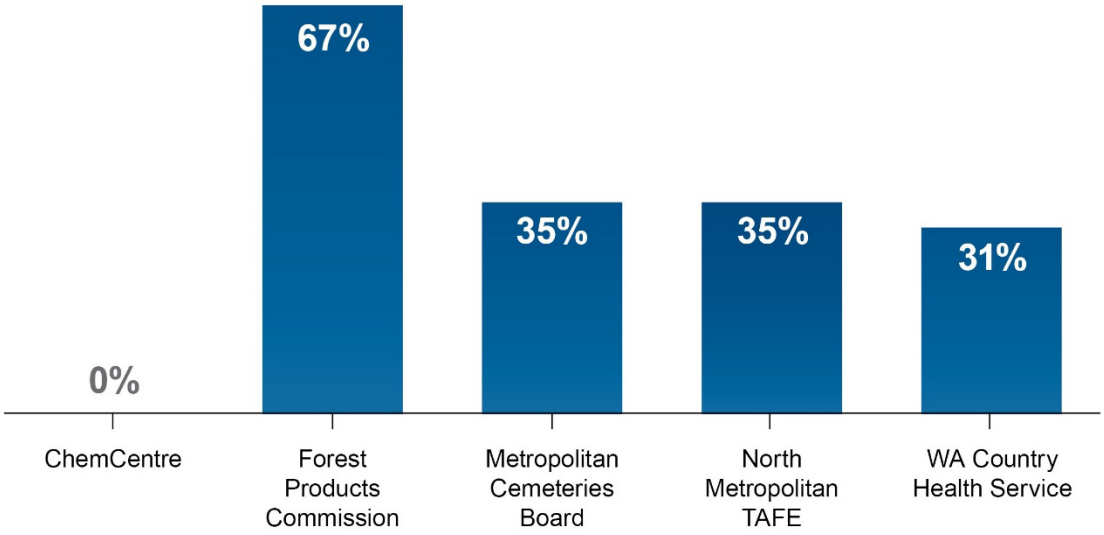
● Standard met ● Standard partially met ● Standard not met

Source: OAG

Table 1: Summary of control effectiveness at audited entities

Entities do not have a good understanding of their portable assets

Four entities do not know the location of all their portable assets. More than a third (34%) of the 115 portable assets we sampled across all entities were not at their recorded locations (Figure 4).



Source: OAG

Figure 4: Percentage of sampled assets not found at recorded location by entity

Some of the assets not found included:

- an ice cream machine at NM TAFE, valued at $3,200
- a telescopic pole pruner at MCB, valued at $1,079
- a spray gun at FPC, valued at $2,284
- a vital signs monitor at WACHS, valued at $4,830.

Entities told us assets could not be located because:

- disposed assets had not been removed from the register
- assets not found during stocktakes are intentionally left on the register in case they are later found. For example, NM TAFE has assets listed in the register that have not been sighted for six years
- assets have been permanently transferred between sites but registers were not updated
- assets are often shared and moved between individuals and locations temporarily without tracking.

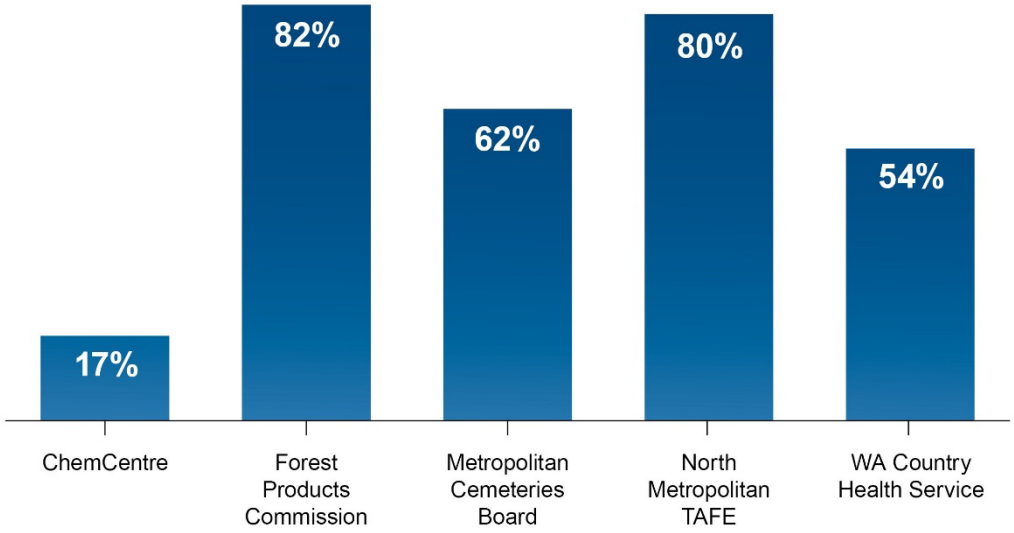
If entities do not accurately track the location of assets, the assets may not be available to assist with service delivery when needed and important information for decision making around maintenance and replacement of assets might not be available.

Entities also did not consistently record portable assets on their registers. Our samples of assets physically sighted onsite and recently purchased assets found:

- 31% of sighted assets were not recorded
- 63% of recently purchased assets[3] were not recorded (Figure 5).

Entities might not know these assets are available for service delivery or when they are due for maintenance and replacement. These assets are also at greater likelihood of being lost or stolen without detection.

[3] New purchases from accounts payable and credit card transactions from the period 1 July 2024 to 30 June 2025. Sampled transactions were more than three months old.



Source: OAG

Figure 5: Percentage of recently purchased sampled assets not on register by entity

Examples of recently purchased assets that were not recorded on entity registers included:

- an e-ink tablet at ChemCentre, valued at $853
- a lawn edger at MCB, valued at $933
- a satellite phone at FPC, valued at $1,181
- a synthesizer at NM TAFE, valued at $1,545
- a telescope at WACHS, valued at $2,830.

Unclear policies (Case study 1), incomplete processes, and lack of regular review and reconciliation of purchases to the register were common reasons why assets were not recorded.

Case study 1: Inconsistent recording of assets on registers

WACHS' policies were unclear on the type of medical assets that had to be registered. This led to the inconsistent recording and understanding of assets available for use.

More than half (54%) of recently purchased portable assets we tested at WACHS were not added to a register, despite similar items being recorded including:

- two telescopes with costs between $2,400 and $2,900
- one ear irrigator/syringe with a cost of $450.

In addition, our sample of physically sighted assets also identified items that were not recorded on the register including, an infant scale and examination light. Similar infant scales on the register ranged in value up to $2,006.

Not all entities conducted regular stocktakes

ChemCentre conduct regular stocktakes of their portable assets to assess the accuracy and completeness of their registers and check the condition of assets. Stocktake practices at the other four entities were mixed:

- FPC did not conduct stocktakes of their portable assets over the audit period.
- MCB had not conducted annual stocktakes of their portable assets as required by their policy. MCB told us it was unable to complete stocktakes due to staff shortages. A stocktake was undertaken in September 2024 which identified registers were inaccurate and assets were missing (Case study 2).
- NM TAFE and WACHS conducted regular rolling stocktakes across all their sites but did not always remove unlocated assets from their registers in case they were later found. In addition, at NM TAFE, the stocktakes did not include all types of portable assets that their procedures require to be physically checked.

Stocktakes help improve the accuracy of asset registers and identify losses which may otherwise go undetected. Long gaps between stocktakes increases the likelihood that loss or incorrect disposal of assets will go unnoticed.

Case study 2: Effective asset tracking impacted by lack of stocktakes at MCB

In September 2024, an MCB stocktake at six cemeteries could not locate 8% (108) of the 1,297 portable assets on its register, despite multiple search efforts. Management approved the removal of all 108 assets from the register as a result of the stocktake.

Inadequate documentation of purchases and disposals, incomplete stocktakes and changes to how they record assets in their finance system were cited as the reasons.

Assets not found included backpack blowers, brush cutters and box trailers.

The assets are essential for cemetery services and maintenance, are easily moved and are often attractive for personal use or gain by on-selling.

Strong controls help to safeguard assets and protect employees from accusations of wrongdoing.

Source: OAG

Figure 6: Photo of backpack blowers at MCB

Entities' disposal practices need improvement

Four entities either had gaps in their disposal policies and procedures or were not following them. Gaps included not covering all types of portable assets, roles and responsibilities not being outlined and a lack of guidance on the storage of assets prior to their disposal to minimise the risk of theft.

We selected 72 portable assets removed from the entities' registers and found:

- 40% of sampled disposal approvals at MCB and 42% at NM TAFE were not authorised by the appropriate manager
- for all 10 disposals sampled at WACHS, disposal method and approval could not be assessed as there was no disposal documentation
- for the 10 disposals sampled at MCB, four did not provide a disposal reason and two a disposal method
- disposal method, reason and approval could not be assessed for 75% of sampled disposals at FPC as there was no disposal documentation.

Inadequate documentation undermines accountability and transparency of disposal decisions and increases the likelihood that unauthorised disposals may go unnoticed.

Staff are guided on the personal use of portable assets to prevent misuse

All entities raised staff awareness of the appropriate use of portable assets, including any allowable personal use. We found:

- ChemCentre and FPC set clear expectations for staff in their codes of conduct and were regularly reminding staff through refresher training

- WACHS and NM TAFE were reminding staff of broad ethical decision-making responsibilities in refresher training but were not as clear on expectations in their codes of conduct
- MCB had clear guidance embedded in asset procedures and in its code of conduct but was not providing refresher training. It started to roll-out a training program during the audit.

Reinforcing staff responsibilities through the code of conduct and training helps to create a culture of accountability and ethical decision making and reduces the risk of portable asset misuse.

Entities have measures in place to deter misuse such as lockable storage, digital keys, asset sign in and out registers, and CCTV. These measures help to prevent staff from inappropriately using assets and ensure they are available for service delivery when needed. Staff are guided to use these measures to secure and protect portable assets.

Recommendations

1. FPC, MCB, NM TAFE and WACHS should improve controls over portable and attractive assets, specifically they should:

    a. review and update their policies and procedures on recording and disposal of portable assets

    b. ensure registers contain sufficient and appropriate information to track portable assets

    c. conduct regular stocktakes of portable assets and keep documentation of stocktake results and reports to management

    d. appropriately document disposal decisions.

    Implementation timeframe: 31 December 2026

    Entity responses: Supported by all entities

Response from audited entities[4]

ChemCentre

ChemCentre acknowledges and thanks the OAG for its review and thoroughness. We are pleased to note that the Report's findings show ChemCentre has met the required standards for effective controls relating to the recording, tracking, and disposal of portable assets. However, ChemCentre will continue to consider opportunities for further refinements and efficiencies in its handling, staff education and oversight of portable assets.

Metropolitan Cemeteries Board

The MCB agrees with the Auditor General's recommendations and acknowledges that control over our portable assets needs to be improved. In particular:

- While the MCB reviewed and updated our procedures in 2025 for the recording, custody and disposal of portable and attractive assets, we commit to reinforcing compliance with these procedures across the agency and are scheduled to conduct a further review of the procedures in 2026.
- Many of the MCB's portable assets, particularly tools used by our ground staff, are based at one location but may be used daily at other sites. The nature of this usage creates difficulties in undertaking stocktakes during working hours and necessitates an improvement in the tracking of those assets during use.
- The MCB commits to undertaking annual stocktakes and commenced the 2025-26 stocktake of our assets in February 2026. With some elements of this stocktake being undertaken outside of normal working hours and instructions to return assets to their recorded location in the register after use, we have noted significant improvements in our ability to locate recorded assets.

With many portable assets subject to significant deterioration through regular use, the MCB commits to improving controls over the disposal of portable assets to ensure the timely update of our register with appropriate supporting documentation.

North Metropolitan TAFE

NM TAFE acknowledges the findings of the performance audit. The organisation is committed to strengthening the management and reporting of low-value and portable assets and will implement the recommendations within appropriate timeframes.

NM TAFE extends its appreciation to the OAG audit team for their professionalism and collaboration throughout this engagement.

WA Country Health Service

WACHS appreciates the independent assurance provided by the Office of the Auditor General and acknowledges the role this oversight plays in supporting accountability and continuous improvement across the public sector. The findings arising from this audit are acknowledged.

WACHS acknowledges the importance of maintaining strong custodial accountability for portable and attractive items. In response to this audit, we are committed to further strengthening organisational controls across all relevant asset categories to ensure effective stewardship, accountability, and compliance with policy requirements.

[4] Forest Products Commission did not provide an additional response beyond agreement to the recommendations on page 14.

Audit focus and scope

The objective of this audit was to assess if five State government entities (ChemCentre, Forest Products Commission, Metropolitan Cemeteries Board, North Metropolitan TAFE and WA Country Health Service) have effective controls over portable assets to minimise loss.

Our criteria were:

1. Are controls to record and track portable assets and their usage effective?
2. Are controls over the disposal of portable assets effective?

During the audit we:

- assessed entities' policies and procedures against legislative requirements, Treasurer's Instructions and guidance
- conducted onsite sample testing to determine the effectiveness of controls to monitor, track and dispose of portable assets, including the accuracy and completeness of registers, at the following sites:
    - ChemCentre – Bentley
    - Forest Products Commission – Harvey and Kalgoorlie
    - Metropolitan Cemeteries Board – Karrakatta Cemetery and Rockingham Regional Memorial Park
    - North Metropolitan TAFE – Joondalup (Culinary Arts) and Leederville (Music and Media)
    - WA Country Health Service – Kambalda Health Service, Coolgardie Health Centre, Harvey District Hospital.
- interviewed entities' staff.

The audit assessed the period 1 July 2022 to 30 June 2025.

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 $351,000.

Auditor General's 2025-26 reports

Number	Title	Date tabled
10	Controls Over Portable Assets – State Entities	6 March 2026
9	Microsoft 365 Security Controls – State Entities	6 March 2026
8	Status of Local Government Audits 2025	28 January 2026
7	State Government 2025 – Information Systems Audit Results	3 December 2025
6	State Government 2025 – Financial Audit Results	3 December 2025
5	Valuation of Property Held by the Public Education Endowment Trust	3 December 2025
4	WA's Progress to Implement the National Principles for Child Safe Organisations (arising from the Royal Commission into Institutional Responses to Child Sexual Abuse)	27 November 2025
3	Maintaining Regional Local Roads	12 November 2025
2	Gold Corporation – Trade Applications	29 October 2025
1	Management of Housing Maintenance Information	6 August 2025

(Appendix AAR: 10.2C)

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

(Appendix AAR: 10.2D)

Office of the Auditor General
Serving the Public Interest

Report 11: 2025-26 | 18 March 2026

PERFORMANCE AUDIT

Local Government Management of Gifts and Benefits

Office of the Auditor General for Western Australia

Audit team:
Jason Beeley
Jordan Langford-Smith
Nayna Raniga
Andrew Harris
Nick Chin

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.

© 2026 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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: shuterstock.com/LightField Studios

(Appendix AAR: 10.2D)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government Management of Gifts and Benefits

Report 11: 2025-26
18 March 2026

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT MANAGEMENT OF GIFTS AND BENEFITS

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 if six local government entities are effectively managing gifts and benefits registers. It also assessed if the Department of Local Government, Industry Regulation and Safety is providing effective guidance to the sector.

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

Caroline Spencer
Auditor General
18 March 2026

Contents

Auditor General's overview 3

Executive summary 4

Introduction 4

Rationale for undertaking the audit 4

Background 4

Conclusion 6

Findings 7

Overall, entities are providing transparency around gifts and benefits 7

Entities are not effectively managing conflicts arising from accepting gifts 11

Entities have policies, procedures and training on gifts and benefits but more support is required 14

Recommendations 17

Response from the City of Bayswater 19

Response from the City of Fremantle 19

Response from the City of Kwinana 21

Response from the City of Mandurah 22

Response from the City of Perth 23

Response from the Town of Cambridge 23

Response from the Department of Local Government, Industry Regulation and Safety 24

Audit focus and scope 25

Appendix 1: Form 4 – Register of gifts 27

Appendix 2: Gifts and benefits better practice guidance 28

Auditor General's overview

Ratepayers and the public have a right to expect that when local government entities make decisions, they are made based on merit and are free from undue influence. This requires entities to have effective policies and practices over gifts and benefits to ensure that there is transparency and that any resulting conflict of interest is appropriately managed. This is a particularly challenging area for council members, whose responsibilities to represent, advocate and build relationships within the community often expose them to offers of gifts and benefits. This audit identified that the range and number of gifts indicates that staff at all levels, not just council members and CEOs, are exposed to the risk of inappropriate influence.

Having complete and accurate gift registers allows scrutiny of who is offering gifts, who is accepting them and whether potentially inappropriate relationships are being cultivated. Our review of the publicly available registers identified that between 2019 and 2024, entities reported over 2,500 gifts valued at approximately $664,000. Event tickets and food and beverages were the most common gifts.

Given some high profile media reporting in recent years, we expected to identify systemic non-compliance with policies and procedures and incomplete recording of gifts and benefits. This was not the case as almost all entities have a gift register and we found evidence of good practice and diligence in the reporting and disclosure of gifts and benefits. Our e-discovery procedures revealed over 900 emails offering gifts and, from that, our detailed review only identified nine gifts above the reporting threshold which were accepted but not recorded within a two-and-half-year period. While there were a further 54 instances where we could not conclusively determine whether a gift was accepted because the staff were no longer employed by the entity, these results highlight the concerted effort entities are taking to transparently disclose gifts and benefits.

Diligent disclosure is important, but so too is managing the conflicts of interest created by gifts and benefits. Significant improvement is needed here as we found many instances where conflicts of interest were not appropriately managed. Across the six entities we audited, 79 individuals had received a gift or benefit from a supplier and had then inappropriately participated in tender assessments, been involved in procurement decisions or overseen contracts with suppliers. This creates unacceptable conflicts of interest which undermine decision-making.

We found that 70% of the gifts at the six entities were accepted by staff and almost half of these were related to events and hospitality. Given this, there is a need for strong controls and clear guidance directed at staff. Entities need to make it clear to potential and current suppliers to not offer gifts, and to staff, that they should decline gifts from current and potential suppliers and proponents.

There is more that the Department of Local Government, Industry Regulation and Safety can do to support entities in meeting their obligations. The six entities we audited all indicated that guidance could be improved, with some seeking independent legal advice to properly understand and meet their obligations. Clear guidance targeted to staff as well as council and CEOs, will help avoid these unnecessary costs being passed onto ratepayers.

Gifts and benefits are a risky and complicated area not just in local government but for all public officials and entities. It is important for all entities to review the findings, recommendations and better practices in this report to ensure that they have strong controls which promote a culture of transparency, impartiality and effective management of conflicts of interest.

Executive summary

Introduction

Following a sector-wide review of publicly available gifts and benefits registers, this audit assessed if the following six local government entities are effectively managing gifts and benefits:

- City of Bayswater
- City of Fremantle
- City of Kwinana
- City of Mandurah
- City of Perth
- Town of Cambridge.

We also assessed if the Department of Local Government, Industry Regulation and Safety (LGIRS) is actively monitoring entity compliance with gifts and benefits regulations and is providing effective guidance to the sector.

Rationale for undertaking the audit

Gifts and benefits can create real or perceived conflicts of interest, impacting integrity and public trust in local government decision-making. Strong governance, clear policies, and effective oversight are essential to manage these risks.

Recent media reports have raised concerns about gift acceptance practices in local governments, including high-value trips funded by external entities. Similar issues have been highlighted in other jurisdictions[1], with audit findings recommending improvements to risk management, policy frameworks and compliance monitoring.

This audit provides transparency over gifts and benefits practices in local government entities, with a detailed examination at six entities.

Background

Managing gifts and benefits is essential for maintaining integrity, accountability and public trust. It helps to prevent conflicts of interest and ensure decisions are made based on merit and not influenced by personal interests.

A gift is something of value given to someone without receiving equal value in return.[2] This can include money, goods, property, travel and hospitality. Benefits are often intangible and include any preferential treatment, privileged access, favours or other advantages offered to an officer above their normal salary or engagement entitlements.[3] Unlike gifts, benefits often

[1] Tom McIlroy, 'Salesforce slammed for lavish gifts meals with NDIA', *Australian Financial Review*, 26 June 2024, accessed 6 August 2024.

[2] A gift is defined within the *Local Government Act 1995 (s5.57)* and includes a conferral of a financial benefit (including disposition of property) made by a person in favour of another person without adequate consideration in money or a travel contribution.

[3] Government of Western Australia, *Managing the Risks of Gifts Benefits and Hospitality*, WA.gov.au website, 15 January 2025, accessed 24 October 2025.

lack a clear monetary value, but they can still create risks, particularly if they appear to offer a private advantage connected to someone's public role.

Gifts and benefits create a connection between the person who gave it and the person receiving it. This might influence how decisions are made, or the perception of how decisions are made. This risk and perception apply to all gifts and benefits, not just those that are required by the *Local Government Act 1995* (LG Act)[4] to be declared.

Although offers of gifts are often provided with positive intentions to recognise working relationships, they can create perceived or actual conflicts of interest and need to be managed based on clear principles that focus on:

- ensuring gifts are declared to provide transparency and enable scrutiny of who is giving and receiving gifts, and why
- considering who benefits from a gift when individuals accept or decline an offer
- declining most offers, particularly those from suppliers or other entities with commercial relationships with the entity
- identifying and managing conflicts of interest to maintain and demonstrate the integrity of decision-making
- good record keeping and active oversight of compliance.

Managing gifts and benefits well relies on individuals being able to do the right thing and make informed decisions. They need support in doing this in the form of codes of conduct, policies and procedures, and training. Gifts can vary widely, from token to substantial. They may be one-off or repeated and may be offered to many people or targeted at individuals. Depending on the context, they may all present a risk and accepting any gift requires careful consideration.

The LG Act regulations require council members and chief executive officers (CEOs) to declare any gift received in their capacity as a council member or CEO valued at $300 or above (or the cumulative value of gifts from one donor if they exceed $300 in a 12-month period) within 10 days of receipt. Council members and CEOs must also manage associated conflicts of interest. The CEO must maintain an up-to-date version of the register and publish it on the entity's official website.

When a council member or CEO receives a gift and the council is discussing a matter related to the donor, the council member or CEO cannot take part in the discussion or decision unless the council or the Minister for Local Government gives them permission to do so. This requirement does not apply to excluded gifts[5].

Mayors, Shire presidents, council members and CEOs are required to represent and promote the interests of their community. This can involve being offered gifts and benefits, particularly invitations to attend events. To manage this, entities under the LG Act are required to have a specific policy covering council member and CEO attendance at events. This policy supports decisions on whether attendance at events should be declared as a gift or whether it is in accordance with the entity's events policy and therefore does not need to be declared.

---

[4] *Local Government Act 1995* ss 5.87A, 5.87B and 5.87C.

[5] Excluded gifts are prescribed under s.5.62(1B) of the *Local Government Act 1995* and includes gifts offered to staff to attend events in accordance with local government rules and policies, gifts offered by other government departments, other local governments or member bodies such as Western Australian Local Government Association and Local Government Professionals Australia.

Local government staff also receive gifts and benefits. However, the requirements for staff differ from the requirements for council members and CEOs. The LG Act regulations prohibit staff[6] from accepting gifts which exceed a $300 threshold in a 12-month period. For gifts below this amount, the regulations require entities to set their own threshold for recording, storing and disclosing gifts accepted by staff in their codes of conduct. This provides flexibility to entities to determine their own reporting requirements for staff.

Given that entities maintain a broad range of commercial or other beneficial relationships, situations may arise that increase the risk of conflicts of interest. It is therefore important that the gifts and benefits staff receive are declared and any associated conflict of interest is managed, although this is not specifically prescribed under the LG Act.

Conclusion

Entities were generally effective in disclosing gifts and benefits, but they need to improve how they manage conflicts of interest from accepted gifts and more support and guidance is needed from the LGIRS. Addressing these weaknesses will help to ensure that decisions are free from undue influence and assist entities in managing their obligations in an efficient and transparent way.

Most entities demonstrated transparency in reporting gifts received by council members, CEOs and staff. All except two of the 147 entities had a published gift register and our e-discovery procedures for unrecorded gifts and benefits at six entities indicated that registers were mostly complete. This transparency is important in maintaining public trust and confidence and helps to ensure accountability in decision-making.

While gift registers were mostly accurate and complete, entities were not effectively managing conflicts of interests arising from accepted gifts. At the six audited entities, there were 79 individuals who accepted gifts from current or future suppliers and were involved with procurement, purchasing or contract management decisions. If conflicts of interest arising from accepted gifts are not managed, decisions may not be free from undue influence.

Current guidance from LGIRS focuses on council members and CEOs, but at the six entities, 70% of gifts were accepted by staff. In addition, current legal and regulatory requirements are out of step with the public sector more broadly, with the thresholds for reporting gifts being high and the timeframes for disclosing gifts being too tight. Clear and appropriate guidance will not only help entities manage their obligations efficiently, but it will also improve the transparency for ratepayers.

[6] For the purposes of regulations 19AB and 19AC of the Local Government (Administration) Regulations 1996, staff are all employees excluding the CEO.

Findings

Overall, entities are providing transparency around gifts and benefits

Almost all entities had gift registers, but some were incomplete or had not been updated, limiting the monitoring of risks and compliance

Although most entities had published gift registers, 78 (53%) entities' registers did not have any information or had information that had not been recently updated (Table 1). Where no gifts or benefits have been accepted, it is important for entities to publish a nil declaration on the gifts and benefits register during the reporting period. Transparency enables the community's ability to scrutinise potential conflicts of interest or undue influence in decision-making.

	Number of entities	Percentage
Did not have published register	2	1%
No data in published register	24	16%
No new data since 1 July 2022	35	24%
No new data since 1 July 2023	17	12%
Published register with current data	69	47%
Total entities	**147**	**100%**

Source: OAG based on public entity data July 2024

Table 1: Review of published entity gift registers

We found that 75% of the registers did not record whether a gift or benefit had been accepted or declined. LGIRS guidelines and Form 4 – Register of gifts (Appendix 1)[7] provided within the regulations to assist entities, does not require this information to be recorded as this is not required by the LG Act and regulations. Tracking both accepted and declined gifts can reveal patterns of attempted influence requiring further oversight.

We note that entities receive many gift offers, including those from community organisations and groups they support. However, declaring declined gifts from commercial entities seeking to benefit from interactions with local governments will help to identify conflicts of interest risks and bring entities more in line with State and Australian entities that report declined gifts.

Decisions to accept gifts and benefits often lack clarity about who the intended beneficiary is. Council members, CEOs and staff did not consistently document details that show consideration of the nature of gifts being offered, why they were offered and in what capacity they were being accepted (for example for official representation, ceremonial purposes or whether personally accepted by staff). Documenting these details and outlining the reasons for accepting or declining gifts or benefits within registers is key. They help individuals demonstrate whether a gift is for their personal benefit, for the benefit of the gift giver, or for the entity they represent. Without these details, ambiguity can lead to inconsistent practices, misinterpretation of regulatory obligations and difficulty in enforcing policies around gift acceptance.

[7] This form is applicable to council members and CEOs.

Entities do not always have the controls and processes to declare gifts within 10 days of receipt as required by the LG Act. Ninety per cent of the registers we reviewed did not record the date the gift declarations were recorded in the register. The absence of this date impairs entities and LGIRS monitoring of compliance with the 10-day rule. This is because most entities are using the Form 4 – Register of gifts (Appendix 1) provided by LGIRS that does not capture this information.

All audited entities are reporting gifts and benefits within their registers, however all indicated that reporting within 10 days of when a gift is received is onerous and impractical. The Australian Government requires its agency heads to report in its registers within 31 days of when a gift is received.[8] We consider this timeframe is more reasonable to allow entities to identify, record and properly communicate decisions and related actions within its registers, whilst continuing to meet public expectations.

Gift registers at the six audited entities were generally complete, providing transparency and allowing for public scrutiny

Dealing with gifts and benefits can be complex, particularly for council members, as their roles in representing, advocating for, and build relationships with the community and stakeholders can lead to offers of gifts and hospitality. Lack of clarity in decision-making can lead to risks, including perceived or actual conflicts of interest, undermining public confidence in the integrity of an entity's operations. While some individuals may assume they are acting appropriately, without a clear framework and principles (Figure 1), policy and code of conduct requirements may not be met, which can unnecessarily damage the reputations of people who aim to uphold high standards in public office.

Source: OAG

Figure 1: Key components of a gifts and benefit framework

Our e-discovery identified just over 900 emails offering gifts and benefits, and from this review we found nine instances where staff accepted gifts that did not match any declaration recorded in the gift register. This reflects a sample of council members, CEOs and staff at

[8] Australian Public Service Commission, *Guidance for Agency Heads - Gifts and Benefits*, ASPC.gov.au, 20 October 2023, accessed 14 July 2025.

each audited entity over a two-and-a-half-year period, and indicates that gifts and benefit registers were generally complete, with three entities having no identified undeclared gifts and benefits. This greatly assists entities to identify, assess and manage conflicts of interest.

The six audited entities confirmed (Table 2) that:

- 48 of the offers were gifts that had been accepted
  - 39 of these were below the $300 threshold limit defined by the LG Act and regulations, or relevant limit for staff[9] and therefore were not required to be declared
  - the remaining nine non-declared gifts have been added to audited entities' gift registers following our enquiries
- a further 197 offers were accepted under the entities event attendance and related policies. These were either paid for by the staff member and therefore not treated as gifts or benefits, or the entity itself paid for them.

Entity	Total number of offers	Gifts that had been accepted	Below the reporting threshold	Above thresholds and now added to the gift register
City of Bayswater	81	27	24	3
City of Fremantle	219	13	13	0
City of Kwinana	106	4	0	4
City of Mandurah	147	0	0	0
City of Perth	294[10]	4	2	2
Town of Cambridge	54	0	0	0
Total	**901**	**48**	**39[11]**	**9**

Source: OAG based on entity data

Table 2: e-discovery results (1 July 2022 to 31 December 2024) identifying offers and accepted gifts by audited entities

In total, the audit resulted in 18 gifts (2%) being added to entity gift registers. Nine of these were above the threshold for reporting and had to be disclosed, another nine were below the threshold but were disclosed voluntarily.

There were another 54 instances (6%) across the audited entities where it could not be determined if the gift or benefit had been accepted or declined because the staff were no longer employed by the entity. In these instances, it is not known if disclosure requirements have been met. However, even if these were all accepted and not disclosed, the level of non-compliance would be low at 63 (7%). The remaining offers were either declined or the entities had paid for the individual to attend an event where a benefit to the entity was identified.

[9] The relevant limit for staff will be the limit prescribed in each entities' code of conduct as required by Regulation 19AC of the Local Government (Administration) Regulations 1996.

[10] Due to the large number of offers, we recommended that the City of Perth focus their review on entries which could raise possible conflicts of interest if accepted. Of the 294 offers identified, 237 lower risk category offers have not been reviewed at the time of this report.

[11] Of these gifts, there were nine that entities voluntarily added nine to the register after the audit.

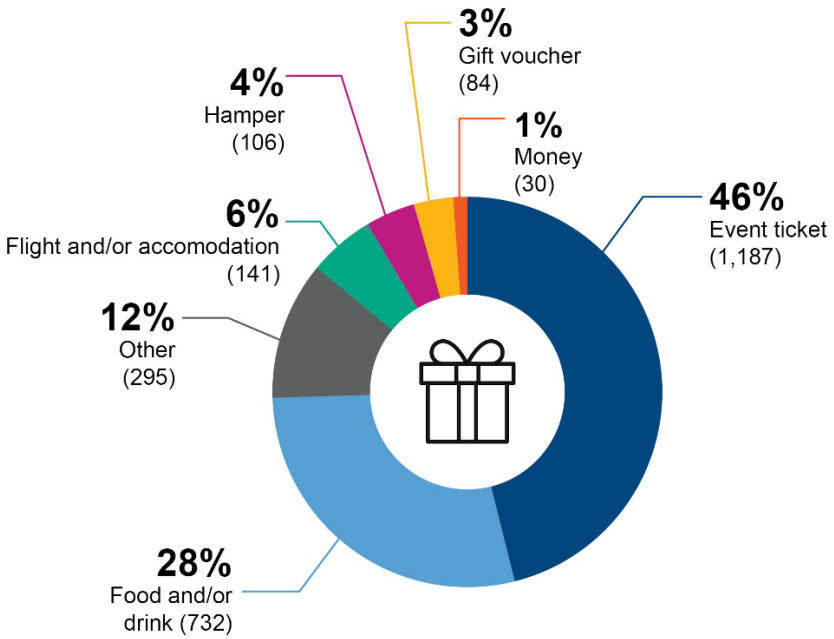
While most of the 48 accepted gifts were work-related and included conferences, hospitality and business-related activities, a small number were accepted for personal benefit. These included a small number of complimentary tickets to VIP sections and corporate suites for sporting events, as well as hospitality (including meals and alcohol). Gifts were accepted from a range of organisations including sport clubs, entertainment/event organisers, professional bodies, mining and IT companies, contractors and suppliers. Accepted gifts and benefits have the potential to create a conflict of interest, even if they are work-related, when they are not identified and managed. This reinforces the need for declarations to detail decision-making to aide with transparency.

The range and number of gifts indicates that staff at all levels, not just council members and CEOs, are exposed to the risk of inappropriate influence

Gifts and benefits are offered and accepted across operational and decision-making roles within entities and by council members and CEOs. While mayors, council members and CEOs receive gifts, staff involved in decision-making areas such as procurement, leasing and property approvals are also offered and accept gifts. These staff are at higher risk of conflicts of interest because of the decisions they make in their roles.

Across the six audited entities, 70% of gift declarations were made by staff. Even though staff have lower reporting thresholds, which can lead to more declarations, receiving gifts still increases the risk of real or perceived conflicts of interest. This shows why strong controls and clear processes for managing gifts are important. These controls and processes should apply at all levels of entities, particularly to high-risk positions.

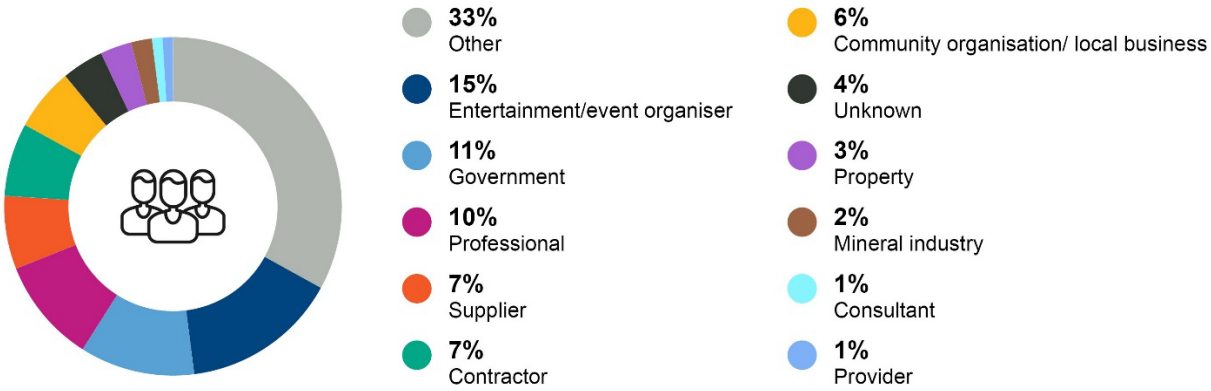
Our review of the publicly available registers of all entities found that between 2019 and 2024 the total number of gifts reported by entities was over 2,500 with a total value of approximately $664,000. Event tickets and food and drink were the most common type of gifts offered, with 10% of all gifts being alcohol and 4% being money or gift vouchers (Figure 2). Gifts of flights and accommodation included 23 instances of international travel.



Source: OAG using publicly available information

Figure 2: Types of gifts recorded in entities' publicly available gift registers between 2019 and 2024

These gifts and benefits were offered by many providers with almost 13% recorded in registers as received from current suppliers and contractors of the entity (Figure 3).



Source: OAG using publicly available information

Figure 3: Sources of gifts recorded in entities' publicly available gift registers between 2019 and 2024

The receipt of gifts and benefits may also be covered by other entity policies and procedures. In accepting gifts, the recipient needs to be mindful of those to ensure compliance with both policies. For example, some member entities of the Perth South West Metropolitan Alliance recorded overseas travel to the United States of America in September 2024 as a gift in their registers and others did not. Where entities have recorded this travel within their gift and benefits registers this provides transparency for council and ratepayers. Entities should still ensure acceptance of gifts and recording of these within gift registers does not substitute for complying with their overseas travel policy requirements.

Entities are not effectively managing conflicts arising from accepting gifts

Conflicts of interest created by accepting gifts are not effectively managed increasing the risk of inappropriate influence

Even when accepted gifts are declared and transparent, we found that the resulting conflicts of interest are not effectively identified or managed. A conflict of interest is created by gift recipients accepting gifts and benefits from current or potential suppliers seeking to obtain work with the entity. We found examples in all audited entities where gifts had been accepted and declared from suppliers but some of these individuals had been involved in procurement decisions or contract management with the supplier. Although in these instances there was a level of transparency about the gifts, because conflicts of interest were not managed, the risk of inappropriate influence was not mitigated.

There were almost 700 instances of accepted gifts or benefits from organisations on the supplier master file for all the audited entities. Of these:

- 79 individuals who had accepted gifts and benefits were then involved in procurement as panel members of tenders, approving procurement decisions and/or purchase requisitions, or overseeing contracts with suppliers
- only five of these individuals (6.3%) had disclosed a conflict of interest risk when participating in a procurement decision relating to the entity providing the gift
- for two of the five individuals, even when a conflict of interest had been declared, we were unable to find any documented strategies to mitigate the risk of influence.

Case study 1 where offers of gifts and benefits from suppliers were accepted by staff. Although the value of the gifts were sometimes small in value, they create a concerning trend as they were identified across the audited entities and resulted in a perceived or actual conflict of interest. If these are not managed, they can lead to the perception of improper influence of decisions made by entities.

Case study 1: Examples of inappropriate gifts offered by suppliers and accepted by staff participating in procurement decisions

- In 2019, a staff member was on the evaluation panel that awarded a contract to a supplier for approximately $111,000. The staff member subsequently managed the contract. Six months before the contract was renewed, the contract manager accepted tickets to watch an AFL game at Optus Stadium. This contract manager was also a panel member during the contract renewal process which saw the contract successfully renewed and increase in value to almost half a million dollars.
- A staff member received three bottles of 12-year-old whisky from a property company valued under $300 after the awarding of a tender for an estimated value of $19.2 million over a five-year period. These gifts were surrendered by the staff member to their social club, and therefore still retained by the entity. The offering and acceptance of such gifts is inappropriate, even after the awarding of contracts, as it is intended to build relationships that may bias future decisions.
- At another audited entity, three staff accepted gifts which included alcohol from a current supplier. Two of the staff were on a tender evaluation panel for that supplier and did not declare any conflict of interest in relation to the gifts. The supplier was the successful tenderer and awarded a contract to the value of $400,000. Those staff have also been involved in approving purchase orders for the supplier.
- At one audited entity the following conflicts of interest were identified and not declared:
    - two staff members accepted a bottle of alcohol each, valued at $50 per bottle from a supplier. One of the staff members approved purchase orders for the supplier and was the nominated representative overseeing the contract, currently valued at $185,000
    - a staff member accepted a bottle of whisky valued at $120 from a supplier and approved purchase orders and purchase amendments from this supplier
    - a staff member received a $50 gift card from a supplier and then went on to approve purchase orders and a contract extension for a further one year for this supplier.
- Thirteen staff at another entity received various $50 gift vouchers in 2019 from a supplier. Four of the staff were involved in the tender process where the gift giving organisation was successful with a contract value of approximately $1.4 million.

All audited entities' policies required panel members to declare conflicts of interest during procurement processes. However, none of them asked panel members when assessing tenders or making procurement decisions to consider whether receiving a gift or benefit may create a conflict. Instead, procurement processes focused primarily on conflicts from personal relationships, proximity, or financial interests, which are better understood by staff and still need to be managed. Staff involved in procurement and commercial activities need to understand conflict of interest risks related to receiving gifts or benefits and when to declare a conflict of interest. By excluding gift-based conflict of interest consideration, entities risk overlooking a key source of influence that can affect decision-making as evidenced in Case study 1.

Conflicts of interest are not considered when recording gifts and benefits, limiting entity oversight of risk and staff compliance with policies

Most audited entities do not require staff to consider the risks from gift acceptance. Five of the six entities' gift registers did not require recipients to consider conflict of interest risks. The City of Mandurah was the only entity that explicitly asked recipients to assess perceived and actual conflict of interest, including whether accepting a gift could lead to a future conflict of interest. Staff are required to consider and document whether the acceptance of the gift creates an impression that the staff member will favour the provider when carrying out their duties. The register also requires declarations to detail information considered in decisions made in accepting or declining gifts, including whether their supervisor or manager has been informed of the gift to aide with oversight, representing good practice.

The City of Mandurah's register is supported by guidance requiring staff to decline the receipt of gifts or benefits from suppliers where conflicts of interest arise and defines which gifts may be acceptable and which are prohibited. Prohibited gifts include:

- any token gift over the value of $50
- any cash or equivalent
- training over $300
- ticket to an event valued over $300
- ticket to an event not related to professional development valued over $50
- any gift of alcohol
- prizes of any value.

Low value gifts can create a perception of bias or preferential treatment if received frequently from parties with vested interests, even when staff are following policies.

The gift registers across the six audited entities showed instances where suppliers and stakeholders offered frequent, low-value gifts such as hospitality, promotional items, and event invitations. While suppliers may wish to showcase the value of their products and services, this should occur through fair and competitive procurement processes – not through gifts. Although low-value gifts often fall below disclosure thresholds and may seem harmless and considered gestures of goodwill, if repeated they can gradually build familiarity and influence over decision-makers. Entities should demonstrate that there is a clear benefit to the entity and not to individuals before accepting the gift.

Some entities have statements of business ethics to help prevent suppliers offering gifts

To minimise staff exposure to the risks from supplier gifts, three of the audited entities have a statement of business ethics (City of Perth, City of Mandurah and Town of Cambridge). A statement of business ethics sets out entity expectations of suppliers in conducting business with them, including not providing or offering gifts and incentives, and provides staff guidance in declining gifts and benefits when offered. At one entity, the implementation of a statement of business ethics resulted in a decline in gift offers from suppliers. A statement of business ethics supports staff to minimise the risk of organisations seeking to influence decisions through gifts and benefits.

However, a statement of business ethics on its own will not always prevent gifts from suppliers. Improvements in policy and procedures, training and monitoring is required to manage the risks of gifts and benefits appropriately.

Audited entities are not using all information to mitigate risks arising from accepting gifts

None of the six audited entities have processes to review information in their gift registers to identify patterns or trends in gifts offered or accepted. This means they are not analysing data that could reveal risks such as offers targeting particular positions, repeated offers from the same company, or conflict of interest risks associated with gift providers. As a result, they are less equipped to identify and address emerging risks.

Further, not all audited entities were using other information they have such as supplier masterfile information, tender registers, lease registers and complaint registers that would help them identify whether controls for gift-based conflicts are working. The City of Kwinana introduced a centralised complaints register, but this has not been implemented long enough to identify trends in conflicts of interest or information which may indicate that there are undeclared gifts and benefits. The other entities could also use complaints information to help identify concerns that relate to fair and transparent decisions. However, these entities did not have centralised complaints information because complaints are dealt with in individual business areas. This siloed approach makes it harder to use the information to identify where there has been at least a perception of a conflict of interest that may be linked to gifts and benefits.

The audited entities rely heavily on staff knowing when to declare gifts and following codes of conduct. Consistent oversight is needed to help entities manage gift declarations. While all the audited entities used an electronic system to manage gift and benefit declarations, there were gaps in recording and ensuring compliance. Two of the audited entities are not fully utilising system functionality with one entity manually recording information between their register and system and the other using their system to only manage council members and CEO declarations. Improving system functionality will help entities ensure the information they have is robust and allow them to use this information for effective oversight of gift and benefit declarations and identify and manage conflicts of interest.

There were six instances across two entities where advice from governance staff to declare gifts was not acted upon, reducing transparency and increasing risk. All audited entities had governance teams providing advice and promoting compliance. In one entity, governance advised staff to return gifts offered by current suppliers, demonstrating proactive support but also highlighting ongoing risks in procurement-related roles. Council members, CEOs and staff are encouraged to seek governance advice when unsure about accepting gifts and leadership teams should support and reinforce the advice governance teams provide. Not following governance advice can undermine transparency and weaken controls designed to ensure compliance and reduce risk.

Entities have policies, procedures and training on gifts and benefits but more support is required

Policies and procedures exist but some are outdated and lack details on what is expected of council members and staff

All six audited entities have policies and procedures to help staff recognise and avoid situations where personal interests could influence, or appear to influence, professional decisions. These policies and procedures are supported by codes of conduct that outline disclosure requirements, but most procedures require improvements to help manage the risks inherent in offers of gifts and benefits.

Four of the six entities' gifts and benefits policies lack clear guidance on when gifts and benefits should be declined, with some being outdated. These entities do not clearly outline examples of prohibited gifts, including not accepting gifts from current or potential suppliers.

This limits their usefulness in helping staff make sound decisions when faced with offers of gifts or benefits and protect the entity from perceptions of bias.

At each of the six audited entities, we saw gifts and benefits being declined by staff, which helps demonstrate that staff do assess and decline gifts when benefits to entities are not clear. Gifts and benefits declined included invitations to sporting events, hospitality that included networking with food and alcohol and gifts offered from suppliers. Some audited entities declined gifts and subsequently chose to pay where a work-related benefit was determined for example where a staff member attended professional development courses. These instances demonstrate staff awareness and the majority try to do the right thing and comply with policy positions.

Policies and procedures clearly define the circumstances when it is appropriate or not to accept gifts or benefits and explain the processes to follow where a perceived or actual conflict of interest exists. The City of Mandurah has published a decision-making tool on its intranet to help convey expectations and guide staff in their decisions and declarations of gifts and benefits. This tool is clear, practical and easy to understand and represents good practice made available by the Public Sector Commission[12] (Figure 4). Guidance to staff also includes the Public Sector Commission's 6Ps and 6Rs Tools[13] for managing conflicts of interest.

G – Giver

Who is providing the gift, benefit or hospitality and what is their relationship to me?

Does my role require me to select contractors, award grants, regulate industries or determine government policies?

Could the giver (person or organisation) benefit from a decision I make?

I – Influence

Is the giver seeking to influence my decisions or actions?

Is the gift, benefit or hospitality being offered to me publicly or privately?

Is it a courtesy, token of appreciation or highly valuable?

Does its timing coincide with a decision I am about to make?

F – Favour

Is the giver seeking a favour in return for the gift, benefit or hospitality?

Is the gift, benefit or hospitality being offered honestly?

Has the giver made several offers to me or people in my business area over the last12 months?

Would accepting it create an obligation on me to return a favour?

T – Trust

Will public trust be enhanced or diminished?

Could I publicly explain why I am accepting the gift, benefit or hospitality?

What would my colleagues, family, friends and associates think?

Have I made good records on accepting the gift, benefit or hospitality in accordance with reporting and recording procedures?

Declining a gift can be as simple as saying "Thank you for your offer however as a public officer it is not appropriate for me to accept gifts".

Source: City of Mandurah

Figure 4: Prompts for City of Mandurah staff to consider when offered a gift (using public sector guidance – decision-making tool)

[12] Government of Western Australia, *Decision-making tool: GIFT test*, WA.gov.au website, 3 November 2021, accessed 25 January 2025

[13] The 6Ps and 6Rs tools help authorities and public officers identify and manage conflicts of interest.

Training is available, but it is often limited to the induction process rather than regularly reinforced to help embed desired behaviours

All the audited entities have formal training covering gift and benefits policies and procedures, but for most audited entities training is provided to council members and staff only during onboarding. The City of Mandurah and the City of Perth provide regular training to staff members, which includes some coverage of gifts and benefits. A lack of regular training reduces the likelihood that the behaviours laid out in policies and procedures are embedded in the culture of entities.

In the absence of regular refresher training, most audited entities rely on seasonal or informal reminders to reinforce gift declaration requirements. These typically occur around festive periods, such as Christmas, or during staff briefings. While helpful, this ad-hoc approach may not provide sufficient guidance for staff to consistently apply policies throughout the year.

LGIRS support and guidance on gifts and benefits is not fully effective

There is limited guidance to the sector for entity staff, leaving entities to develop their own guidance, increasing the risk of inconsistent practice across the sector. LGIRS guidance, last reviewed in 2022, is targeted only to council members and CEOs as they are explicitly covered by the LG Act and regulations. LGIRS supports entities and responds to specific individual queries on gifts and benefits but does not proactively communicate these more broadly to enable shared learning.

In some areas the LGIRS guidance has not been sufficient, resulting in different interpretations by entities. Some entities were obtaining their own independent legal advice, at the cost of ratepayers, to help them meet their compliance requirements. In one instance LGIRS recommended an entity seek their own legal advice if they had any doubt on LGIRS interpretation of a query they raised with them. This query was in relation to the timing of exactly when a gift was accepted. Without clear guidance, inconsistent practice can lead to limited transparency and make monitoring of compliance by LGIRS difficult.

All the audited entities told us the guidance provided by LGIRS is not sufficient to meet their needs. For instance, the current disclosure requirements do not require declarations of declined gifts and the disclosure threshold of $300 is higher than that set for the WA State and Australian government entities ($50 and $100 respectively). This can restrict transparency and may not reflect community expectations. All audited entities have independently set lower value thresholds than those required, indicating the $300 threshold does not meet their risk tolerances.

Recommendations

To enable effective management of gifts and benefits, entities should:

1. provide education and guidance that sets out entity expectations and assists staff and council members in making decisions by:
    a. implementing clear and up to date policies and procedures that outline gifts that are acceptable (good practice limits these to token gifts)
    b. requiring accepted and declined gifts from commercial entities, be declared
    c. specifically outline gifts that are prohibited
    d. implement regular training and education programs to ensure staff understand and apply policy, procedure and code of conduct, in practice and when making decisions.

    Implementation timeframe: December 2026

    Entity response: Entities generally accepted the recommendations but noted that there is currently no legal or regulatory requirement to disclose declined gifts.

2. Implement fit for purpose, risk-based monitoring and reporting mechanisms to:
    a. proactively oversee gift and benefit declarations
    b. analyse information across the entity to identify undeclared gifts, check that controls are working and identify any concerning trends or patterns
    c. manage perceived and actual conflicts of interest, requiring these declarations to consider the receipt of gifts and benefits
    d. consider a centralised complaints register to highlight where controls and processes have not been followed and identify systemic risks.

    Implementation timeframe: December 2026

    Entity response: Recommendation supported.

To enable effective oversight of compliance requirements and in supporting the local government sector, LGIRS should:

3. review regulatory requirements and guidelines to consider:
    a. reducing the $300 threshold or explaining why it remains appropriate (noting state entity requirements of $50 or Australian Government requirements of $100)
    b. increasing the timeframe for updating gift registers from 10 days to better reflect the tempo and nature of senior attention, decision-making and compliance reporting processes, (noting 31 days is the Australian Government timeframe)
    c. amending the Form 4 template to record both the date the gift was received as well as the date the gift register was updated to allow regulatory compliance to be monitored.

    Implementation timeframe: December 2026

    Entity response: Recommendation to be considered as part of review of potential legislative reform and updates to guidelines.

4. Issue updated guidance and templates to the sector to:

   a. extend guidance beyond elected members and CEOs to include all entity staff

   b. require entity gift registers to disclose accepted gifts and benefits and declined gifts from commercial entities to:

      - improve transparency – listing all offers improves trust that declined gifts have not been accepted informally and staff have not been subject to influence
      - improve compliance - declined gifts can help identify patterns where repeated offers from the same person or company are being offered or identify situations requiring further oversight
      - help protect staff by officially recording declined gifts demonstrating compliance and maintaining trust.

   Implementation timeframe: December 2026

   Entity response: LGIRS accepts the recommendation.

Response from the City of Bayswater

The City of Bayswater thanks the Office of the Auditor General (OAG) for its comprehensive report. We acknowledge the complexity of this audit and appreciate the significant effort involved in reviewing extensive information to develop recommendations that support local governments in managing gifts and benefits effectively.

The report confirms that local governments are generally complying with legislative requirements. The data reflects robust governance practices and strong adherence to these requirements, providing confidence in overall compliance across the sector.

Three gifts were identified as accepted by City of Bayswater employees, but not recorded in the City's Gift Register. Two related to an Economic Development Breakfast and one to an Awards Ceremony where the City was nominated for an award. Employees were requested to attend these events as part of their official duties and therefore did not perceive or identify them as gifts.

The City acknowledges there is always room for improvement. While the findings confirm a strong commitment to integrity and sound governance practices, the City of Bayswater values the recommendations and remains committed to continuous improvement and maintaining high standards of accountability.

Response to Recommendations:

Finding 1: The City will review and update its processes and training to provide enhanced education and guidance on the management of gifts and benefits.

Due Date: 31 December 2026

Finding 2: The City will implement a risk-based approach to monitoring the recording and reporting of gifts and benefits.

Due Date: 31 December 2026

Response from the City of Fremantle

Recommendation 1

All newly elected Council Members at the City of Fremantle are required to complete an induction and mandatory training following the election. The City's induction process includes a presentation from WALGA or City Officers, outlining their role and responsibilities as an Elected Member, this includes gifts and interest disclosure requirements. They are also provided with an induction manual, which includes various information regarding gifts and disclosure of interest requirements. The induction manual also includes operational guidelines published by the Department, Council policies and procedures. In 2025, the city also introduced an internal intranet site for Elected Members to provide them with direct access to up-to-date information relevant to their role.

Officers at the City are required to complete mandatory Code of Conduct training, which includes important information in relation to gifts, and specifically outlines that gifts over $300 are prohibited. Information regarding disclosure of interest relating to gifts has also been included in the City's new procurement policy, guidelines and mandatory training. Officers are reminded that they are required to disclose any interests relating to a supplier when undertaking any procurement process such as an RFQ or Tender. Online and in person Governance training has been implemented to ensure staff are aware of their

requirements relating to gifts, and regular reminders and information is also published on the City's internal intranet site.

Elected Members and staff are required to disclose gifts in accordance with the requirements of the Local Government Act and these disclosures are recorded within a gift register which is published on the City's website. The City has not implemented the requirement to disclose gifts that have been declined, as this is not a requirement of the Act. However, staff are required to record this information in the City's records keeping system for future reference.

Recommendation 2

In addition to the annual Compliance Audit Return review, the City undertakes regular internal Governance audits, to monitor gift disclosures and compliance. When non-compliance occurs, the matter is reviewed and appropriate action is taken. This may include mandatory training relating to gift and interest disclosures, or if the matter is serious or repeated, disciplinary action may be taken and the matter is reported to the Department and CCC. If non-compliance is related to an Elected Member or the CEO, this is reported to the Department and CCC as required.

Disclosure of declined gifts

Whilst the City makes every effort to ensure Staff and Elected Members are aware of their requirements relating to gifts, and gift disclosures are made to ensure compliance and transparency, in the City's opinion, the disclosure of gifts that are declined is not required for the following reasons:

The Local Government Act 1995 establishes disclosure obligations for gifts that are received by the CEO and Council Members. Section 5.87A(1) requires disclosure only for gifts that have been received. The term "received" implies acceptance and possession of the gift. Where a gift is declined, it is never taken into possession and therefore does not meet the statutory condition of being "received". As such, a gift that is offered but not accepted, in the City's opinion, does not fall within this definition.

The intent of disclosure provisions is to ensure transparency regarding benefits that may influence decision-making. If a gift is declined, no benefit is conferred, and therefore no potential for undue influence exists. Recording declined gifts as disclosures could create unnecessary administrative burden and misrepresent the nature of interactions, as no actual transfer of value occurred. Therefore, a gift that has not been accepted should not be disclosed, as it does not meet the legislative requirement of being "received," nor does it present any risk of influence or conflict of interest.

Gifts received electronically by email

A gift offered via email is not considered "received" until formal acceptance occurs. The City's interpretation is based on the following principles:

Section 5.87A of the Act requires disclosure of gifts that are received. The term "received" implies both acceptance and possession. An emailed offer is merely an invitation; until the recipient formally accepts, no transfer of benefit has occurred. The intent of the legislation is to ensure transparency regarding benefits that may influence decision-making. If a gift remains unaccepted, there is no actual benefit conferred, and therefore no potential for undue influence.

Formal acceptance provides a clear, auditable point in time when the gift becomes a reportable item. This prevents ambiguity about whether an offer constitutes a received gift and supports consistent governance practices. Treating emailed offers as "received"

without acceptance could lead to unnecessary disclosures and misinterpretation of interactions. Requiring formal acceptance ensures that only genuine transfers of value are recorded.

In conclusion, a gift offered by email should only be considered “received” once formal acceptance has been given, as this aligns with the statutory wording, legislative intent, and best practice for transparency and accountability.

Concluding remarks

As a result of this Audit, the City has commenced a review of the information, processes and training provided to staff and Elected Members relating to gift and disclosures of interest, to ensure improvement. Various initiatives as outlined in the responses above have already been implemented, and additional improvements are being considered by the City, with the intent to be implemented as actions as a result of this audit. These actions will be reported to the City’s Audit, Risk and Improvement Committee for consideration and adopted by Council.

Response from the City of Kwinana

The City of Kwinana (City) appreciates the Office of the Auditor General’s (OAG) report on local government management of gifts and benefits and supports the recommendations provided. The City values the OAG’s review and acknowledges the importance of robust compliance practices in relation to gifts, benefits and conflicts of interest. The findings and insights outlined in the report will assist the City in further strengthening its ongoing commitment to transparency, integrity and public trust in decision-making.

The report highlights that legislative change alone may not always achieve all governance outcomes as intended. It reinforces that compliance with minimum statutory requirements does not necessarily equate to best practice. The City recognises the OAG’s encouragement for local governments to exceed baseline standards, including consideration of measures such as declaring declined gifts and recording supplementary information in the Form 4 register. While the City acknowledges the value of enhanced disclosure, the inclusion of additional information is not currently within the scope of the legislatively prescribed form. Accordingly, the City suggests that any expansion of reporting requirements be supported by formal legislative amendment and that proposed changes be clearly communicated to all local governments to ensure consistent application.

The City is committed to supporting its Governance and Legal team in the implementation of required changes arising from the OAG’s recommendations. The Leadership team will play a key role in proactively promoting clear information and encouraging adherence to updated processes and procedures, ensuring that all staff are well-informed and equipped to comply effectively. The City also notes its support for the recommendations directed to the Local Government Integrity Reporting System (LGIRS).

Since the OAG audit commenced in November 2024, the process has already prompted improvements to the City’s internal practices concerning gifts, benefits and conflicts of interest. The City has initiated a comprehensive review of relevant processes and is progressively implementing necessary changes. A detailed project plan has been developed to guide the coordinated implementation of all recommendations. Progress reports will be provided to the City’s Audit, Risk and Improvement Committee for ongoing oversight and monitoring.

The City will continue to implement these improvements with the objective of maintaining best practice standards in the management of gifts, benefits and conflicts of interest. The

City thanks the Office of the Auditor General for its audit and constructive recommendations and is confident that the actions underway will further enhance governance, accountability and community confidence.

Recommendation 1

The City acknowledges and accepts the recommendations outlined for the effective management of gifts and benefits, and conflicts of interest within Local Government entities. Since the commencement of the OAG audit, the City has proactively begun implementing changes to its approach.

Recommendation 2

The City acknowledges and accepts the recommendations regarding the implementation of fit for purpose, risk-based monitoring and reporting mechanisms. The City would like to note it has completed recommendation 2(d) by establishing the City's "Feedback Register" in August 2023.

Response from the City of Mandurah

The City of Mandurah (the City) has established controls in place that address the OAG recommendations. These controls are reviewed annually to assess their effectiveness and to support continuous improvement.

Through the City's control environment, employees are required to carefully assess the appropriateness of accepting any gift or benefit, particularly where they are involved in procurement activities, grant assessments, or the exercise of delegated authority.

Employees are reminded that the acceptance of a gift must not compromise, or be seen to compromise, their impartiality or the integrity of the City. Decisions must be made on merit, free from undue influence. Where there is any doubt, employees are required to decline the gift and/or seek guidance in accordance with the City's Code of Conduct requirements.

The City has a number of controls to proactively oversee gifts and benefit declaration, including quarterly and annual reporting.

The City will improve its current reporting to the Chief Executive Officer to include a three-year trend analysis that will identify: number of gifts received; number of gifts offered and declined; individuals repeatedly receiving gifts; business units repeatedly receiving gifts; suppliers repeatedly offering gifts and categories of gifts received. Where there a trends observed, the City will utilise this information to provide:

- further education for individuals or teams;
- improvement to controls, such as procedures and guidelines;
- contact City suppliers regarding their obligations under the Statement of Business Ethics, i.e. do not provide gifts to City employees.

The City will further strengthen its employee gifts and conflict of interests training, including identifying and managing any actual, potential or perceived conflict of interest arising from it. This requirement will apply particularly where employees are:

- Undertaking procurement and tender evaluation processes
- Assessing or recommending grant funding
- Exercising delegated or statutory authority

- Training materials, guidelines and procedures will be updated to reinforce these obligations and ensure consistent understanding and application by City officers.

The City will continue to reinforce these obligations through, training, guidelines and ongoing awareness initiatives to ensure consistent and ethical decision-making across the organisation.

Response from the City of Perth

The City of Perth is committed to continuous improvement and feedback and has welcomed the opportunity to participate in the OAG's Local Government Management of Gifts and Benefits Audit.

The City has a range of policies and guidance in place for both staff and elected members to support them in meeting their obligations relating to the declaration of gifts and benefits. This also provides additional guidance and oversight in the management of any related interests.

Based on the two recommendations in this report the city will further enhance its education and training on gifts and benefits and interests' management.

Recommendation 1

The City of Perth believes it already has clear and up to date policies in place. However, the City will review its gifts management framework to ensure currency and promote best practice. The City will also continue to encourage its Elected Members to declare all gifts.

The City is developing additional training (face to face) to further support employee understanding of gifts management at the City. Additional training (face to face) is expected to be implemented in the first quarter of 2026.

Recommendation 2

The City of Perth will review its gifts management framework to ensure currency and promote best practice as suggested in this report. Noting that Employee and Elected Member complaint registers will continue to be kept separately.

Response from the Town of Cambridge

The Town of Cambridge is committed to continuous improvement and has welcomed the opportunity to participate in the OAG’s management of gifts and benefits performance audit. The Town acknowledges the overall findings and recommendations and supports the better practice guide.

The Town has maintained strong internal controls in relation to the acceptance of gifts and benefits. In addition, our outward facing Statement of Business Ethics clearly establishes the Town’s expectations in relation to the conduct of business with the Town, including not offering gifts.

The Town will look to incorporate the better practice system of controls detailed in the report as part of a future review of the Town’s policy and procedures in relation to the acceptance of gifts and benefits.

Response from the Department of Local Government, Industry Regulation and Safety

Recommendations 3 and 4

Suggested legislative reform would need to be considered as part of the larger reform program and would be subject to stakeholder consultation and decisions of Government.

LGIRS acknowledges the Auditor General's observation and supports the need for clear and practical guidance to assist local governments in managing integrity risks.

Our current guidance is directed at council members and CEOs, as they are explicitly covered by the regulations. Gift disclosure and reporting requirements for local government employees that are not CEOs should be included in each individual local government employee code of conduct. LGIRS recognises that additional guidance may assist local governments in supporting staff to meet the requirements of their codes of conduct.

The Local Government Regulatory Approach outlines LGIRS' commitment to fostering best practice and supporting compliance across the sector. Consistent with this approach, LGIRS issued a Local Government Alert – Guidance on managing gifts, benefits and hospitality on 4 September 2025, encouraging all local governments to review their codes of conduct and consider additional policies. LGIRS will continue to engage with the Western Australian Local Government Association and the Local Government Professionals WA to review its guidance materials and to explore opportunities for further sector support, including joint training initiatives by 31 December 2026.

LGIRS notes that the Local Government Inspector formally commenced on 1 January 2026. This represents a significant change in the State Government's regulatory approach for the local government sector, and accordingly, the Local Government Inspector will play a central role in shaping the future compliance framework and approach to proactive monitoring. LGIRS will liaise with the Local Government Inspector to hand over this recommendation for consideration as part of the Inspector's compliance monitoring plan. LGIRS will also engage with the Inspector regularly to assist with monitoring.

Audit focus and scope

This audit was conducted with an initial review of published gifts and benefits registers from all 147 entities with results informing our more in-depth work at six metropolitan entities.

The objective of this audit was to assess whether entities effectively manage gifts and benefits.

We based our audit on the following criteria:

- Are entities complying with their gifts and benefits policies and procedures?
- Are entities recording all offers of gifts and benefits?
- Are entities' decisions for accepting or declining gifts and benefits appropriate?
- Are entities recording and managing all conflicts of interests in relation to gifts and benefits?
- Is LGIRS actively monitoring compliance with the regulations and providing adequate guidance to entities?

The audit reviewed gifts and benefits registers and the recording and management of conflict of interests at each audited entity over the period 1 July 2019 to 30 June 2024.

We assessed each entity's policies and procedures against legislative requirements, LGIRS' operational guidelines and our better practice guidance in Appendix 1. At each entity, we also:

- reviewed policies, procedures and processes relating to gifts and benefits
- examined records and processes for monitoring conflicts of interest
- reviewed all entity / regional council entities' gifts and benefits register for council members, CEO and council
- conducted e-discovery procedures on the email correspondence of selected key decision makers for undeclared gifts and benefits to test the completeness of gift and benefit declarations
- e-discovery procedures used defined terms of common offers of gifts and benefits we identified through our initial review of published gifts and benefits registers of all entities. Our results are restricted to these terms meaning not all offers of gifts and benefits to selected risk positions can be identified
- where e-discovery procedures identified offers of gifts and benefits, these have been assessed by entities. They have updated their registers to record and make transparent gift offers that have been accepted and notified external entities where compliance obligations were not met
- reviewed tender and procurement contracts
- met with key staff from governance, procurement, contracts and finance areas.

We did not assess electoral gifts as they fall under different rules and regulations and are only relevant for a specific period (during elections).

It is outside the scope of this audit and our remit under the *Auditor General Act 2006* to, and we did not, conduct any investigation of:

- the conduct of any individual member of staff in accepting gifts or benefits or the appropriateness of each individual decision to accept a gift or benefit
- the appropriateness of decisions made by staff after accepting gifts or benefits
- the conduct of any commercial supplier; or
- whether there was any direct or deliberate attempt to influence any particular procurement by offering gifts or benefits to entity staff or seek to identify any direct inappropriate influence on any specific procurement.

As this was our first audit into gifts and benefits for local government entities, we are not naming individuals and have relied on the sampled entities to update their gift registers and report non-compliance appropriately. However, we may change this position in future audits if we again find instances where gifts and benefits are accepted, but not disclosed.

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 $690,000.

Appendix 1: Form 4 – Register of gifts

Local Government Act 1995

Local Government (Administration) Regulations 1996

REGISTER OF GIFTS

Name of person making disclosure	Description of gift	Name and address of person who made gift	Date gift was received	Estimated value of gift at time it was made	Nature of relationship between person who made gift and person who received gift	For a gift that is a travel contribution — description and date of travel	For an excluded gift under s. 5.62(1B)(a) — the date of the approval referred to in s. 5.62(1B)(a)(ii) and the reasons for the approval

Source: Local Government (Administration) Regulations 1996

Form 4 – Register of gifts within the Regulations to be used by entities to manage risks associated with the receipt of gifts and benefits highlighted weaknesses.

Appendix 2: Gifts and benefits better practice guidance

Entities need to have gifts and benefits policies and procedures that are up-to-date and accessible to staff. These policies and procedures should include key controls for the declaration of gifts and benefits, the management of conflict of interests created from accepting gifts and benefits and regular review and monitoring.

The table lists the key elements of a system of controls for effective gifts and benefits management, which guided our audit.

Key elements / Framework component[14]	Outcome	What we expect to see
Policies and procedures	Comprehensive, approved and up-to-date policies and procedures to provide all local government staff with guidance on their obligations	• clear and easy to understand policy and procedures that detail prohibited gifts • code of conduct signed at start of employment and annually thereafter • clear and specific definitions of gifts and benefits to aid in decision-making and limit ambiguity, providing examples relevant to entity operations • set out overarching entity expectations reinforcing policy, procedures and code of conduct messages • management of gifts and benefits considered in the context of ethical conduct, impartiality, honesty, transparency and accountability • evidence of periodic review.
Declaration of all gifts and benefits	Consistent expectations	• all gifts and benefits are declared regardless of value or acceptance • standardised declaration forms, ensuring consistency of information recorded and decision-making process • consider whether the receipt of gifts and benefits results in a conflict of interest that needs to be identified and managed • gift registers should detail where there are nil returns to ensure they provide transparency and date of update of registers should be evident
Making appropriate decisions	Clear decision-making framework	• to minimise risk, the entity's policy position should be communicated to stakeholders, suppliers and clients – his could include sharing the statement of business ethics • guidance to aid staff with decision-making and when the acceptance of gifts may be considered appropriate • guidance be clear in setting out processes for avoiding and managing conflicts of interest to

[14] Refer to Figure 1 Key components of a gifts and benefits framework

Key elements / Framework component[14]	Outcome	What we expect to see
		consider who benefits from the acceptance of the gift or benefit • decisions be based on risk assessment that consider potential, perceived and actual conflicts of interest • provide clear guidance on declaring conflicts of interest, managing (with documented mitigation strategies) and reviewing these • guidance to support staff in declining gifts and benefits.
Training and education	Training to increase awareness of impartiality, integrity and conduct expectations	• regular codes of conduct, fraud awareness and integrity training (yearly) • regular reminders to council members, CEO and staff to make sure there is awareness and understanding of compliance obligations • advanced integrity training for staff in areas identified as high risk of influence (e.g. procurement, recruitment, finance, binding decision makers).
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 Identification of patterns, areas of increased risk Evidence of reviews should be retained	• reports from monitoring and reviews made available to leadership and audit committee periodically • all accepted and declined gifts or benefits reported to a central member of management to allow for effective oversight • monitor for repeat offers and cumulative value as these may flag risk where there is an intention to influence decisions that require further scrutiny, as well as monitor acceptance of repeat token gifts that may otherwise go undetected.

Key components of a gifts and benefit framework

Identify and record gifts and benefits

Identify and manage conflicts of interest

Use information to monitor and oversee risk

Source: OAG

This page is intentionally left blank

Auditor General's 2025-26 reports

Number	Title	Date tabled
11	Local Government Management of Gifts and Benefits	18 March 2026
10	Controls Over Portable Assets – State Entities	6 March 2026
9	Microsoft 365 Security Controls – State Entities	6 March 2026
8	Status of Local Government Audits 2025	28 January 2026
7	State Government 2025 – Information Systems Audit Results	3 December 2025
6	State Government 2025 – Financial Audit Results	3 December 2025
5	Valuation of Property Held by the Public Education Endowment Trust	3 December 2025
4	WA's Progress to Implement the National Principles for Child Safe Organisations (arising from the Royal Commission into Institutional Responses to Child Sexual Abuse)	27 November 2025
3	Maintaining Regional Local Roads	12 November 2025
2	Gold Corporation – Trade Applications	29 October 2025
1	Management of Housing Maintenance Information	6 August 2025

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

(Appendix AAR 10.2E)

Office of the Auditor General
Serving the Public Interest

Report 12: 2025-26 | 25 March 2026

INFORMATION SYSTEMS AUDIT RESULTS

Local Government 2025

Office of the Auditor General for Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Michael Chumak
Khubaib Gondal
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.

© 2026 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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: OAG

(Appendix AAR 10.2E)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government 2025 – Information Systems Audit Results

Report 12: 2025-26
25 March 2026

This page is intentionally left blank

(Appendix AAR 10.2E)

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT 2025 – INFORMATION SYSTEMS AUDIT RESULTS

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 of the *Auditor General Act 2006*.

Our information systems audits focus on the computer environments of entities to determine if their general computer controls effectively support the confidentiality, integrity and availability of information systems and the information they hold.

This is our seventh report on general computer controls (GCC) audits for local government entities. The purpose of GCC audits is to evaluate how well entities' computer controls safeguard the integrity, confidentiality and availability of key financial business systems.

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

Caroline Spencer
Auditor General
25 March 2026

Contents

Auditor General's overview 3

2025 at a glance 4

Introduction 5

Conclusion 6

What we found: Capability maturity assessments 7

What we found: General computer controls 9

1. Access management 10

2. Information security framework 11

3. Endpoint security 11

4. Human resource security 13

5. Network security 13

6. Business continuity 15

7. IT operations 15

8. Risk management 16

9. Change management 16

10. Physical security 17

OAG insights and tips 18

Resources 20

Appendix 1: Capability assessment benchmark 21

Appendix 2: Year-on-year capability assessment result comparison (11 entities in 2024) 22

Auditor General's overview

As part of our annual financial audits, my office reviews local government entities' general computer controls to determine if they effectively maintain the integrity, confidentiality and availability of key business systems and information. At selected entities, we also conduct capability maturity assessments that rate entity controls against our benchmark.

Our 2025 audits highlight ongoing challenges for entities to strengthen their IT governance and security. While it was positive to see the number of entities that had control weaknesses reduce to 68 this year (89 in the prior year), 60% of our findings were unresolved issues from prior years. Entities need to address these persistent control weaknesses to safeguard their important systems, information and service delivery.

Our capability maturity assessments at 15 entities saw an overall decline in all 10 control categories, in part due to four new entities being included for the first time. The 11 entities assessed previously generally stayed in line with prior year levels in four categories and declined in six. We intend to gradually increase the number of entities subject to capability maturity assessments to gain further insights and assist with continuous improvement in the sector.

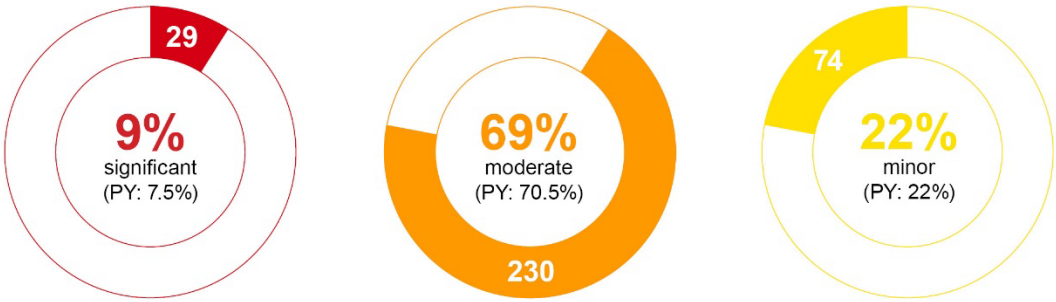
This report highlights some particularly concerning results, such as only one entity meeting the benchmark for access management and two for endpoint security. It also includes case studies highlighting good and bad practices as well as resources that entities can use for further guidance. I encourage the entire local government sector to learn from these and implement effective controls, many of which do not require costly technology. Instead, uplift requires an ongoing awareness of risk and constant vigilance and effort.

2025 at a glance

333 findings at **68** entities (PY: 360 at 89 entities)
60% of findings were unresolved from prior years

Capability maturity model at **15** entities (PY: 11 entities)

Snapshot of controls and findings



General computer controls	Control categories	Capability maturity assessments	
78 findings to 36 entities (13, 52, 13)	Access management	7% of entities met the benchmark	-20%
61 findings to 49 entities (8, 37, 16)	Information security framework	20% of entities met the benchmark	-16%
48 findings to 28 entities (3, 43, 2)	Endpoint security	13% of entities met the benchmark	-5%
23 findings to 19 entities (12, 11)	Human resource security	47% of entities met the benchmark	-8%
18 findings to 16 entities (2, 12, 4)	Network security	33% of entities met the benchmark	-22%
41 findings to 35 entities (3, 30, 8)	Business continuity	27% of entities met the benchmark	-18%
20 findings to 13 entities (8, 12)	IT operations	60% of entities met the benchmark	-4%
19 findings to 19 entities (15, 4)	Risk management	60% of entities met the benchmark	-40%
17 findings to 17 entities (13, 4)	Change management	53% of entities met the benchmark	-29%
8 findings to 8 entities (8)	Physical security	47% of entities met the benchmark	-17%

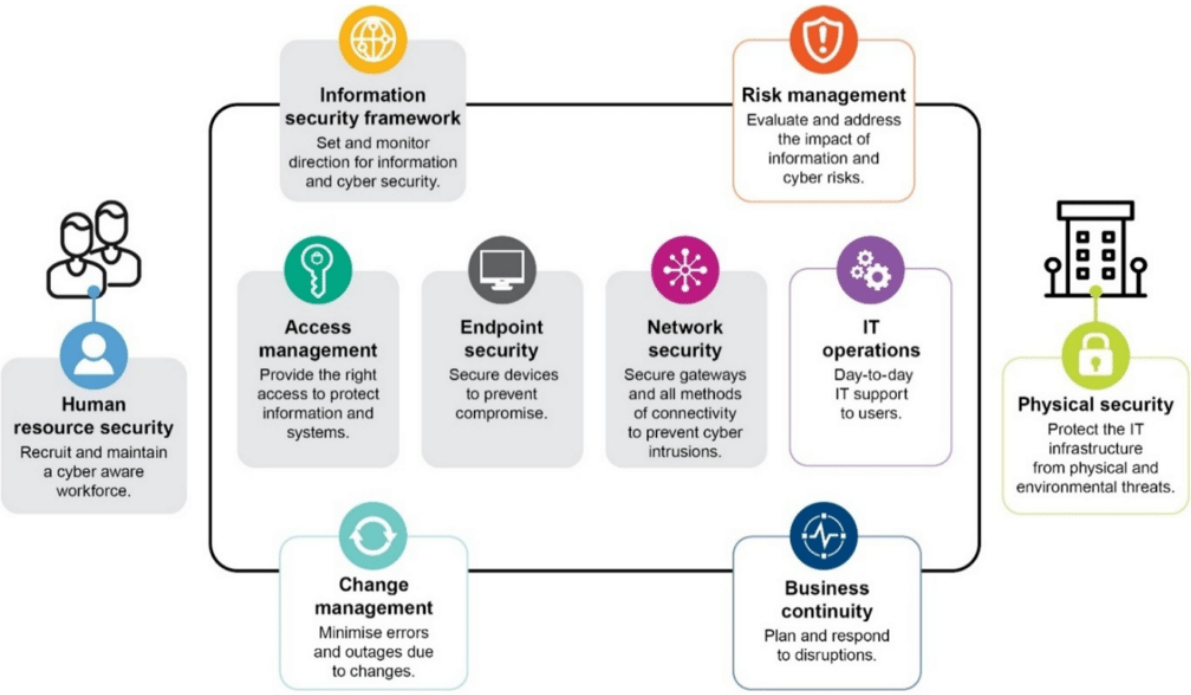
These five categories relate to **information and cyber security controls**

Note: the control categories are ordered from most to fewest findings.

Introduction

This is our seventh report on general computer controls (GCC) audits for local government entities. The purpose of GCC audits is to evaluate how well entities' computer controls safeguard the integrity, confidentiality and availability of key financial business systems.[1] This requires auditors to understand entities' IT environments and associated risks.[2]

For the 2025 year, we reported GCC weaknesses to 68 entities. We also provided 15 of these entities with a more in-depth capability maturity assessment. These assessments evaluate the maturity and effectiveness of entities' IT controls across our 10 control categories (Figure 1).



Source: OAG

Note: shaded categories relate to information and cyber security.

Figure 1: Audited control categories

Our audits incorporate recognised industry standards and better practices such as ISO 27002[3] and the Australian Signals Directorate's *Strategies to mitigate cybersecurity incidents*[4] which include the Essential Eight. They also consider entities' business objectives, complexity of computer systems and the information they hold.

[1] Auditing and Assurance Standards Board, *Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement*, AUASB, February 2020, accessed 24 April 2025.

[2] Auditing and Assurance Standards Board, *The Consideration of Cyber Security Risks in an Audit of a Financial Report*, AUASB, May 2021, accessed 24 April 2025.

[3] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection – information security controls*, 2022.

[4] Australian Signals Directorate, *Strategies to mitigate cybersecurity incidents*, Australian Cyber Security Centre website, n.d., accessed 2 April 2025.

Conclusion

Entities have addressed some prior year findings, but many weaknesses remain unresolved, particularly those related to information and cyber security controls. These weaknesses put entities at greater risk of service disruptions, disclosure of ratepayers' data, financial loss and reputational damage.

We reported 333 control weaknesses to 68 entities in 2025, compared to 360 weaknesses to 89 entities the year before. Nine per cent were rated significant, 69% moderate and 22% minor. The majority (60%) of the weaknesses were unresolved issues from prior years. The average number of findings remained in line with the prior year.

The capability maturity assessments we conducted at 15 entities show ongoing challenges in building effective information and cyber security capability. The maturity levels have stagnated or deteriorated across all 10 categories, with most entities failing to meet our benchmark.

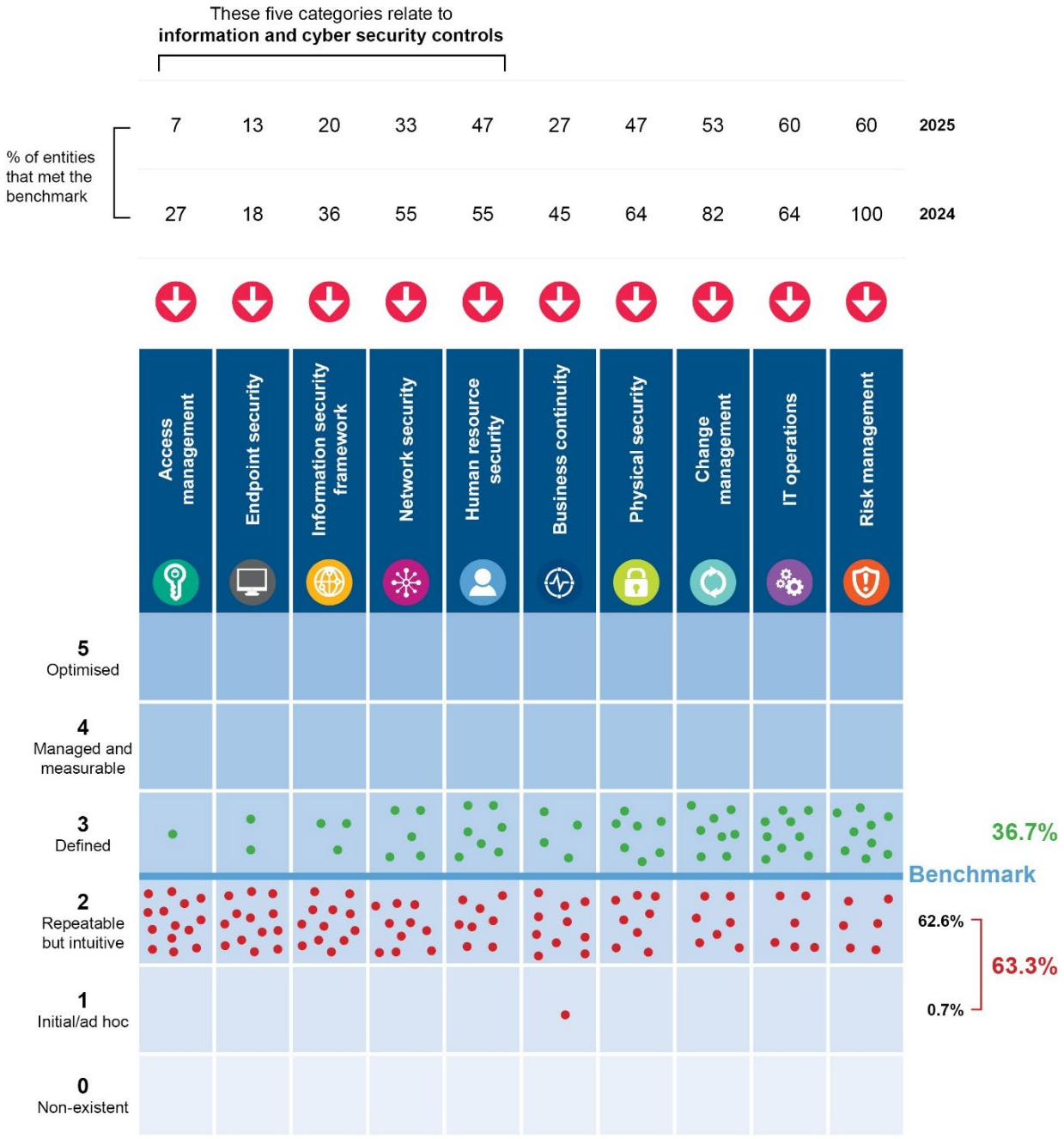
Identified control weaknesses collectively increase the risk of incidents that could compromise the integrity, confidentiality and availability of entities' key systems and information.

What we found: Capability maturity assessments

In 2025, we conducted capability maturity assessments at 15 entities. We assessed entities' capability maturity levels across 10 categories on a 0-5 scale (Appendix 1), with a level of three or higher required to meet our benchmark. These categories include controls that play a key role in maintaining entities' security posture.

There was a decline in the maturity levels in all 10 categories compared to the prior year (Figure 2). The four entities we assessed for the first time this year contributed to this decline. The remaining 11 entities on average stayed in line with prior year levels in four categories and declined in six (Appendix 2).

Although most entities had policies and procedures for risk management, we identified that entity controls to mitigate risks were not operating effectively. As a result, this category showed the sharpest drop in 2025, followed by change management, network security and access management. This is of concern, as strong risk and change management practices are vital to proactively identify, assess and mitigate potential threats and reduce the likelihood of disruptions due to technology updates. Weak network security and access management practices can further adversely affect the integrity, confidentiality and availability of financial systems and sensitive information.



Source: OAG

Note: each dot represents an entity's maturity in the control category, ordered from lowest to highest performing (left to right).

Figure 2: Capability maturity assessment results

What we found: General computer controls

We reported 333 general computer control weaknesses to 68 entities across the 10 control categories (Figure 3). Nine per cent of the findings were rated significant, 69% moderate and 22% minor. Most of the weaknesses were rated moderate and can expose the entities to cyber threats if left unaddressed.

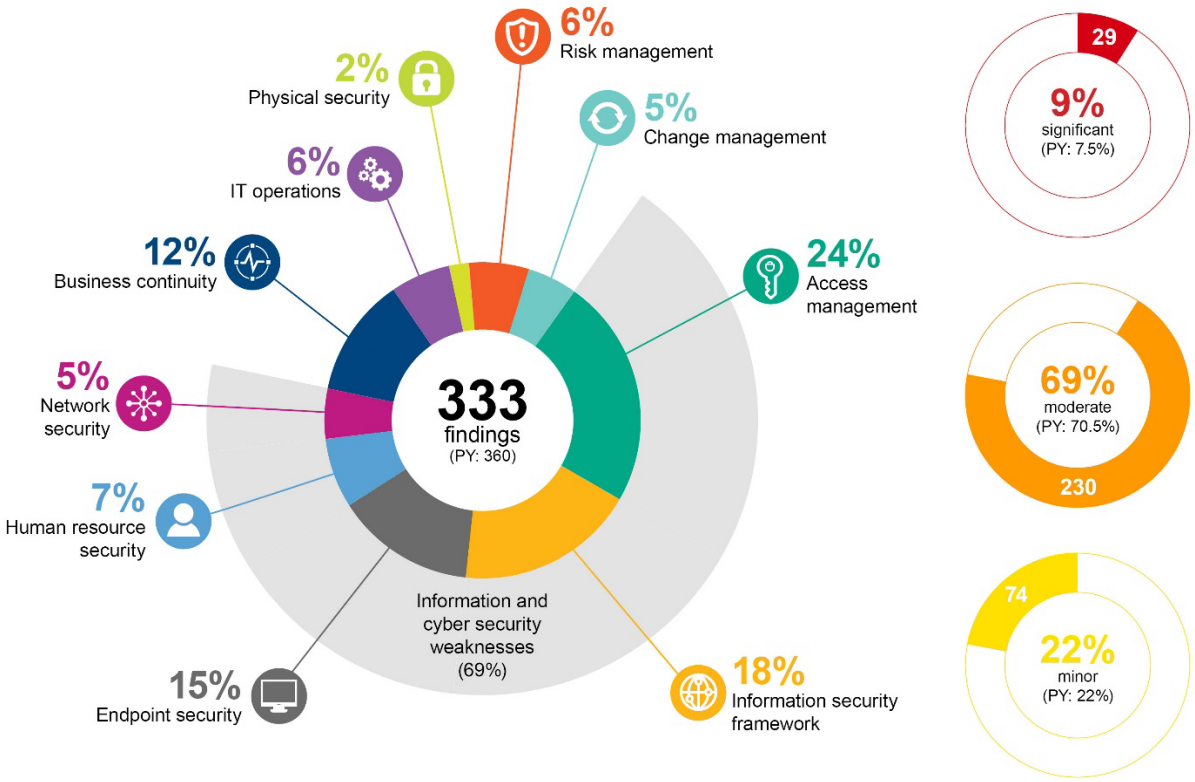
While the overall number of weaknesses has reduced since last year, the average number of weaknesses per entity remains largely the same.

The following control categories had significant weaknesses:

- access management
- business continuity
- endpoint security
- information security framework
- network security.

Most of the weaknesses, including significant, were unresolved issues from prior years. Of the significant issues, two thirds were identified as significant previously and the remaining third elevated to significant in 2025.

Throughout this report, case studies demonstrate how weak controls can compromise the integrity, confidentiality and availability of entities' essential systems and information.

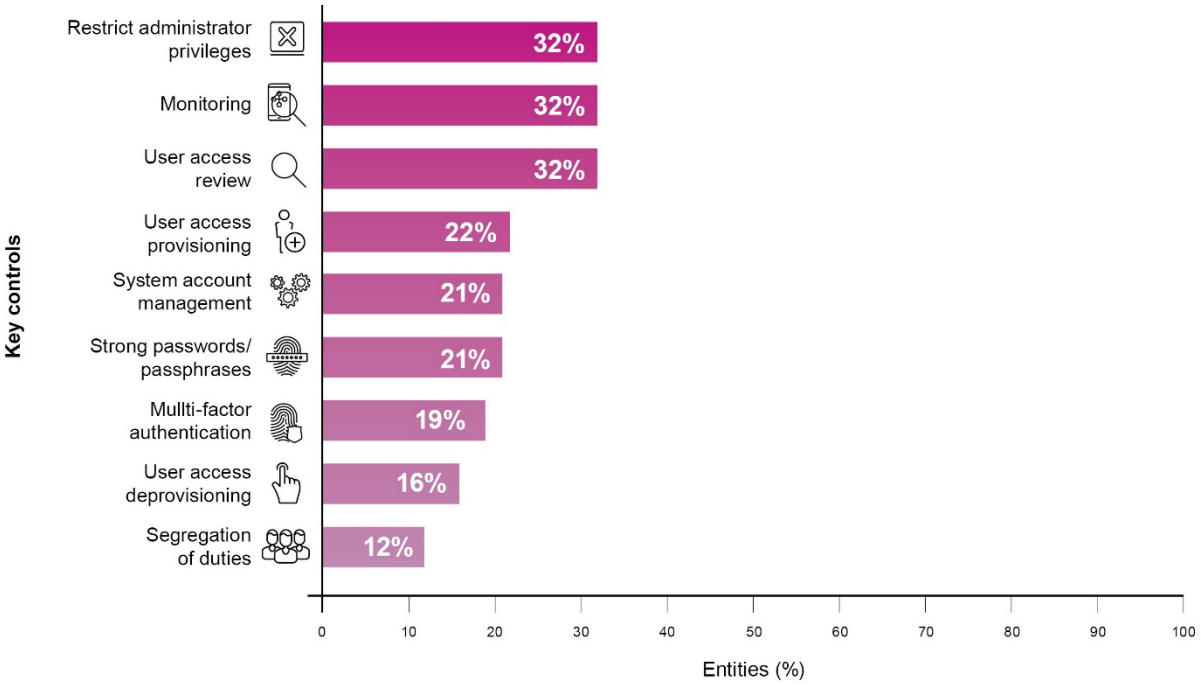


Source: OAG

Figure 3: Ratings and distribution of GCC findings

1. Access management

Access management continues to be an area of concern with the highest number of weaknesses (78) reported to 36 entities: 17% were rated significant, 67% moderate and the rest minor. Over half of these weaknesses (59%) are unresolved from the prior year.



Source: OAG

Figure 4: Percentage of entities with key access management control weaknesses

Nearly one-third of the entities lacked effective controls over administrator privileges, user activity monitoring or regular reviews of user access. These weaknesses increase the likelihood of data breaches. We also continue to identify poor password practices and lack of multi-factor authentication. Entities must prioritise strong authentication to achieve an effective layer of defence.

The following case studies highlight weaknesses we reported to entities and the potential impacts.

Case study 1: Weak database controls

An entity was not logging or auditing changes made directly to data in its finance and human resources database, had not encrypted sensitive information and did not have a dedicated database administrator.

These weaknesses create a risk that data manipulation could occur without detection, making it impossible for the entity to trace or hold individuals accountable for such actions.

Case study 2: Lack of multi-factor authentication for remote administrator access

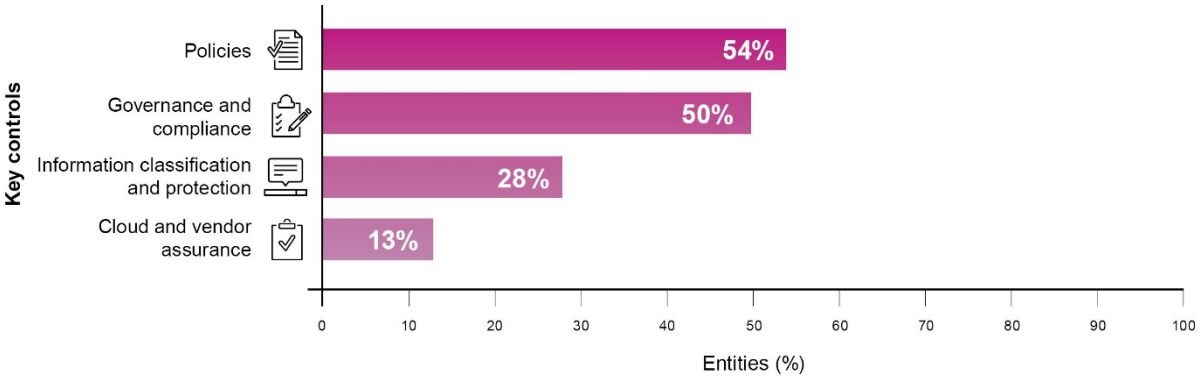
An entity did not require multi-factor authentication for remote access, increasing the likelihood of compromised accounts being used to target the entity network. Remote connections were also permitted for highly privileged accounts, such as domain administrators. It is better practice to limit remote access to standard user accounts to reduce the potential damage in the event of a breach.

Case study 3: Permanent privileged access to human resources application

An entity had permitted an external vendor permanent privileged access to its HR application through a shared account. This included permissions to edit payroll information and other personal details of entity staff. If privileged access is not restricted to just-in-time, it becomes difficult to monitor and trace actions performed by third parties, especially when shared accounts are used.

2. Information security framework

We reported 61 weaknesses in this category to 49 entities: 13% were rated significant, 61% moderate and 26% minor. Most of weaknesses (74%) were findings unresolved since the prior year.



Source: OAG

Figure 5: Percentage of entities with key information security framework control weaknesses

Most entities lacked effective and up-to-date policies to govern, manage and protect their information and technology environments. We found further weaknesses such as lack of an ICT steering committee to oversee and provide strategic direction for ICT initiatives, at half of the entities.

The following case study highlights a good practice we observed at one entity.

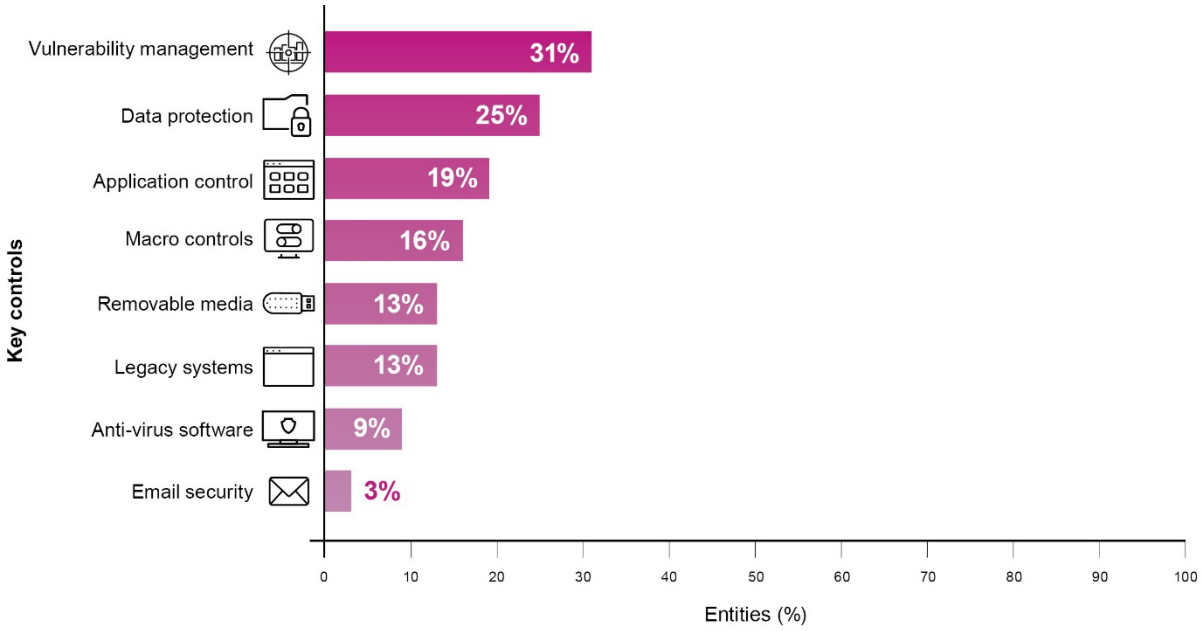
Case study 4: Good controls to prevent data loss

An entity has implemented appropriate controls for data loss prevention. These controls generate alerts when the transfer of personally identifiable and sensitive information is detected. Staff were also prevented from accessing the entity's cloud services from unmanaged devices (e.g. personal computers and mobiles not enrolled in the entity's system).

Strong data loss prevention measures help keep personal and sensitive information safe from unauthorised access.

3. Endpoint security

We reported 48 weaknesses in this category to 28 entities: 6% were rated significant, 90% moderate and the rest minor. Most of the weaknesses (63%) were unresolved from prior years.



Source: OAG

Figure 6: Percentage of entities with key endpoint security control weaknesses

Entities often failed to promptly identify, assess and patch vulnerabilities, and updates to legacy systems[5] were deferred. Insufficient controls to mitigate malware and known vulnerabilities further increased the risk of security breaches.

The following case studies highlight a good practice and a weakness we observed.

Case study 5: Good oversight over vulnerabilities

An entity is managing its patching activities well. It reviews its scheduled patch deployments and compliance across its environment. Proactive patch management lets the entity understand how effective its patching operations are and identify areas of improvement. The entity is better prepared to protect itself from software vulnerabilities.

Case study 6: Ineffective Microsoft Office macro controls

An entity did not appropriately configure controls to restrict Microsoft Office macros.[6] We found over 70% of entity staff could run macros.

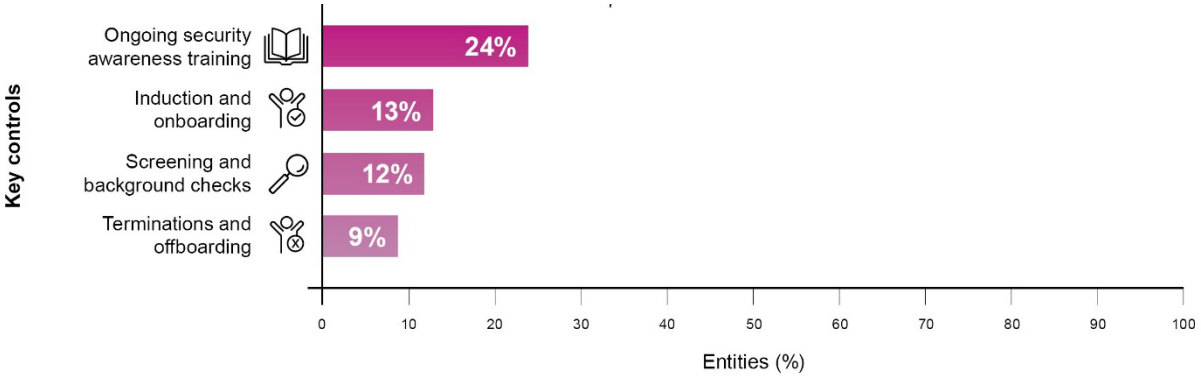
Macros are a common channel for malware attacks which can affect the confidentiality, integrity and availability of entity systems and information. Entities should minimise the use of macros and only allow it for legitimate business needs.

[5] A legacy system no longer receives support, including security updates, from the vendor. It should be transitioned to an up-to-date, supported system to improve security.

[6] Microsoft Office macros are software code used to automate repetitive tasks.

4. Human resource security

We reported 23 weaknesses in this category to 19 entities: 52% were rated moderate and 48% minor. This area continues to demonstrate ongoing issues, with most weaknesses (65%) remaining unaddressed from previous years.



Source: OAG

Figure 7: Percentage of entities with key human resource security control weaknesses

Entities had insufficient security awareness training. This increases the likelihood of successful phishing and impersonation from staff not detecting suspicious activity or understanding practices for safeguarding data. Entities also failed to carry out proper onboarding and background checks.

Effective human resource security controls reduce the likelihood of insider threats and cyber criminals taking advantage of staff through social engineering.

The following case studies highlight weaknesses we reported and their potential impacts.

Case study 7: Phishing results in fraudulent payment

An entity was subject to a successful social engineering attack resulting in account details of a supplier being changed in their finance application. Approximately $350,000 was paid to an unknown third party before the breach was discovered. Effective security awareness training often acts as the first line of defence against social engineering attacks such as this. Entities should ensure all staff undertake training periodically.

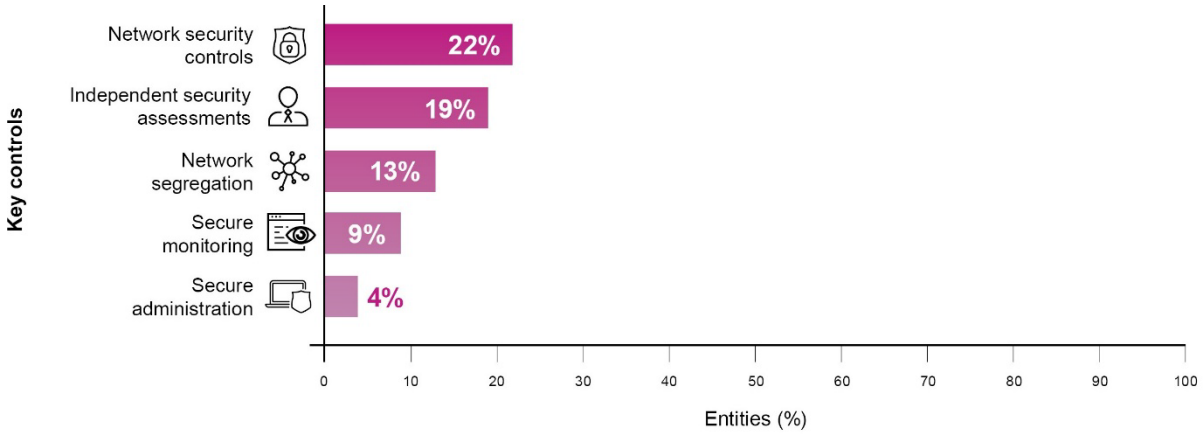
Case study 8: Failure to seek police clearances

An entity did not perform police clearance checks on sampled key staff in privileged roles, such as a senior management accountant, finance officer and systems administrator. Lack of police clearance checks could lead to an entity inadvertently hiring people that increase the likelihood of sensitive information and asset theft or misuse.

Entities should perform appropriate background screening, including police clearance checks, for positions of trust to assess the risks and make informed decisions about granting access to their systems and information.

5. Network security

We reported 18 weaknesses in this category to 16 entities: 11% were rated significant, 67% moderate and the rest minor. A third (33%) of the weaknesses in this area were unresolved prior year findings.



Source: OAG

Figure 8: Percentage of entities with key network security control weaknesses

Weaknesses in this category were mainly due to weak network security controls, which are crucial in safeguarding critical systems against cyber threats. Other weaknesses included insecure management of network devices, ineffective network segregation and a lack of control over unauthorised devices. Entities were also not regularly testing their controls through penetration testing.

The following case studies highlight a good practice we observed as well as weaknesses we reported to entities and the potential impacts.

Case study 9: Continuous external security assessments provide better protection

An entity assesses its IT environment and infrastructure continuously, focusing on firewall configuration, network penetration tests and its implementation of the Essential Eight mitigation strategies. Continuous assessments allow the entity to accurately track the effectiveness of its controls and help maintain strong cyber security defences, reducing the risk of security breaches.

Case study 10: Default passwords and poor network security expose building management system

An entity had not changed the default credentials for administrator access to their building management system. This vulnerability, combined with the entity's weak network and endpoint controls, could allow attackers access to systems managing temperature, lighting and doors.

Entities should use strong passwords for critical systems, keep operational technology networks separate from corporate networks and block unauthorised device connections.

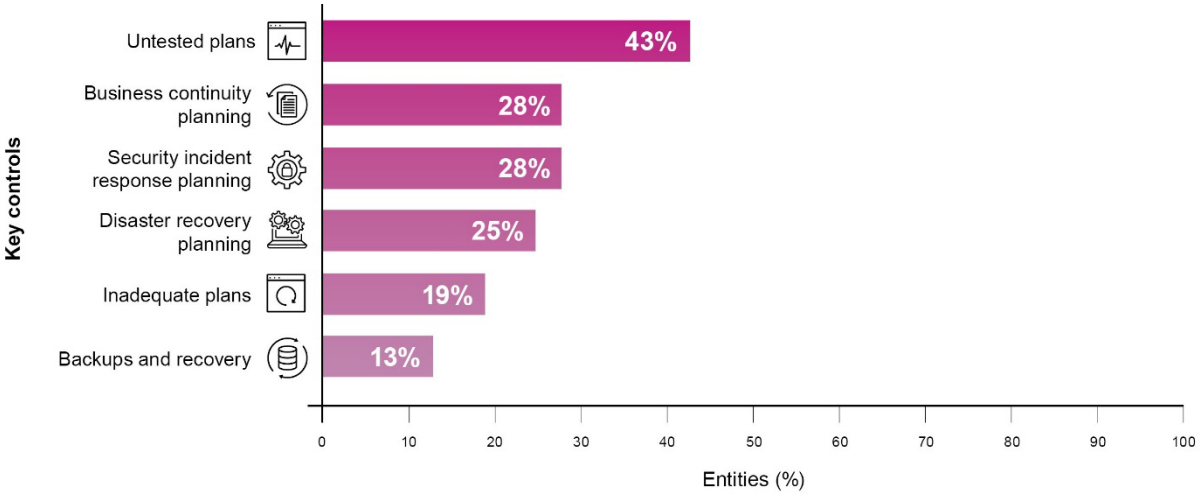
Case study 11: Lack of network security allows corporate network access from public computers

An entity did not restrict network traffic between its critical servers and its publicly accessible areas effectively. Through our testing, we could establish a connection to its critical servers from the public library. Poor network controls significantly heighten the risk of compromise.

Entities should restrict traffic between networks effectively to safeguard the confidentiality, integrity and availability of their systems and information.

6. Business continuity

We reported 41 weaknesses in this category to 35 entities: 7% were rated significant, 73% moderate and the rest minor. Most of the weaknesses (61%) were unresolved from prior years.



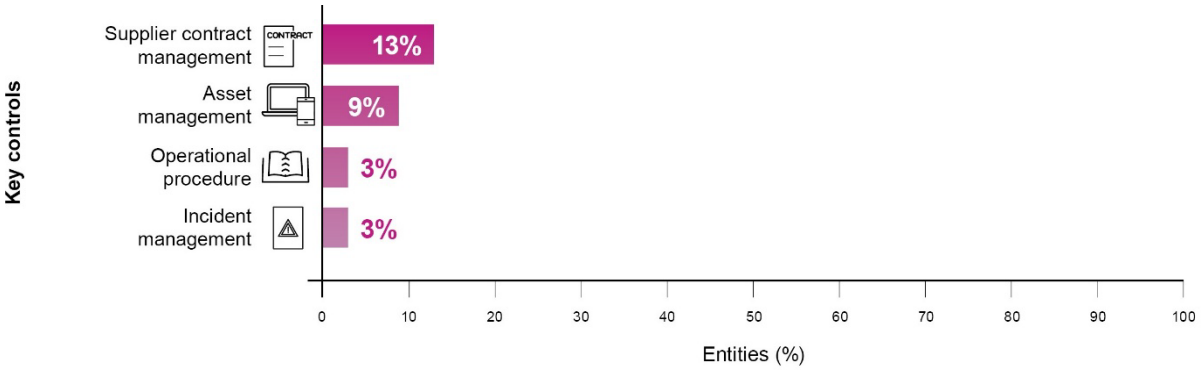
Source: OAG

Figure 9: Percentage of entities with key business continuity control weaknesses

Most weaknesses in this category resulted from entities not testing business continuity and disaster recovery plans regularly. As a result, plans are often outdated and lack proper validation through testing. Disasters, though rare, can greatly affect business. Without up-to-date, well-documented and tested plans, entities may struggle to manage incidents and restore services promptly.

7. IT operations

We reported 20 weaknesses in this category to 13 entities: 40% were rated moderate and 60% minor. Although entities generally performed well in this category, half of the weaknesses were unresolved issues from the prior year.



Source: OAG

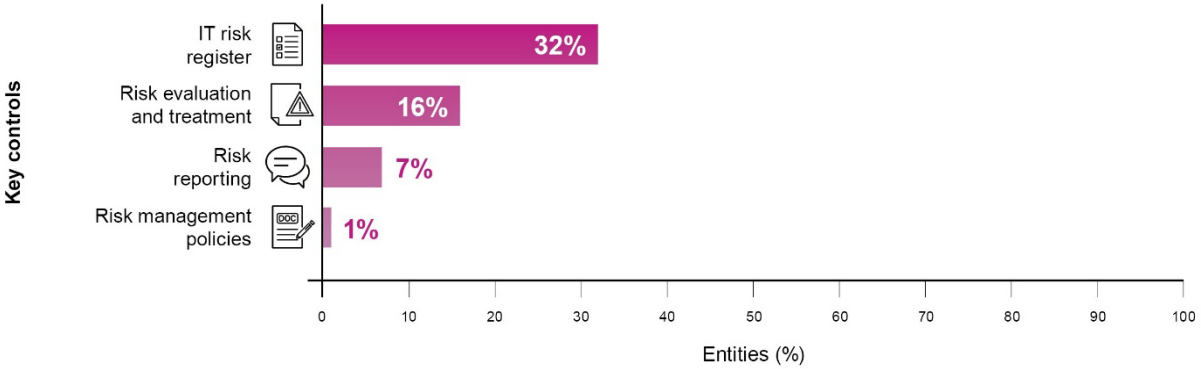
Figure 10: Percentage of entities with key IT operations control weaknesses

Most weaknesses were due to entities either not having well-documented cyber security requirements in supplier contracts or poorly managed service level agreements. Weak IT asset management practices at some entities also increased exposure to potential financial or information loss.

The IT operations category focuses on services delivered to entity staff. Operational disruptions, poor asset management or ineffective service desk processes could directly affect users' productivity, lead to loss of IT assets and compromise of data.

8. Risk management

We reported 19 weaknesses in this category to 19 entities: 79% were rated moderate and the rest minor.



Source: OAG

Figure 11: Percentage of entities with key risk management control weaknesses

Most of the weaknesses we identified related to incomplete or outdated IT risk registers. We also found discrepancies in entities' control effectiveness assessments, where controls did not mitigate risks effectively.

The following case study highlights a weakness we reported and its potential impact.

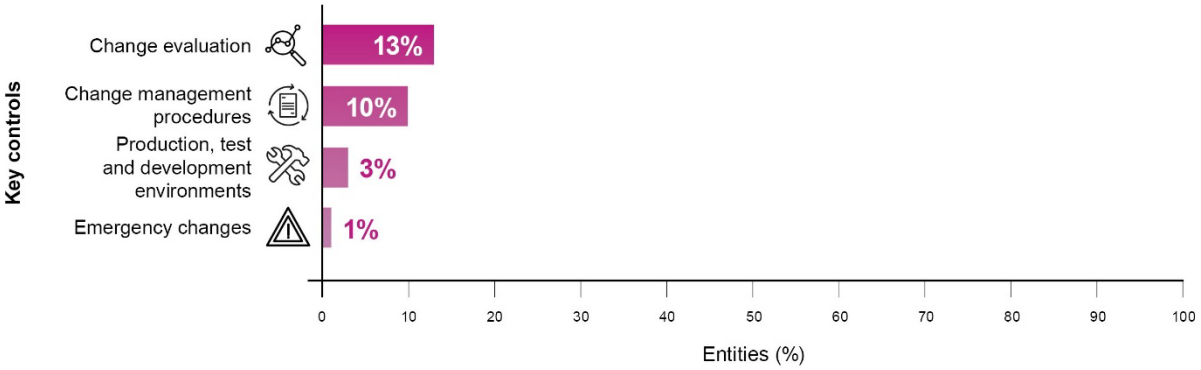
Case study 12: Inadequate oversight over IT risks

An entity did not review, monitor and report identified IT and cyber security risks, mitigation strategies and controls. A lack of appropriate IT risk oversight can result in greater risk to business plans and information security over time.

Entities should ensure that identified IT and cyber security risks are reviewed regularly and are in line with their risk management plans.

9. Change management

Entities generally performed well in this category. We reported 17 weaknesses to 17 entities: 76% were rated moderate and the rest minor.



Source: OAG

Figure 12: Percentage of entities with key change management control weaknesses

Our testing found issues with change control weaknesses, including changes made without proper evaluation and incomplete or ad hoc change records. Poor change management can result in system outages and service disruptions.

The following case study highlights a weakness we reported and its potential impacts.

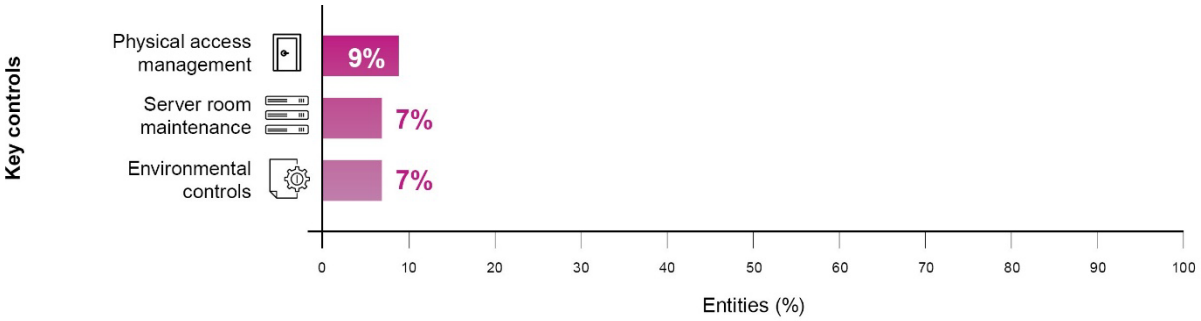
Case study 13: Lack of separate development and test environments increases operational risks

An entity did not maintain development and testing environments for one of its key business applications. All updates were applied directly in production without testing, impacting live data and increasing the risk of service disruptions.

Entities should use separate environments for safer changes to critical applications.

10. Physical security

This is another category where entities tend to perform well. We reported eight moderate-rated weaknesses in this category to eight entities.



Source: OAG

Figure 13: Percentage of entities with key physical security control weaknesses

The identified weaknesses were due to inadequate management of physical access controls for buildings and server rooms, such as granting excessive privileges or failing to revoke access in a timely manner. Furthermore, some entities failed to keep proper conditions in their server rooms putting IT equipment at risk of being damaged.

The following case study highlights a weakness we reported and its potential impacts.

Case study 14: Fire risks in server rooms

An entity's server rooms lacked fire suppression systems and the fire-rated walls had structural damage. The entity was also storing old, unused IT equipment in one of the server rooms. These factors increase the potential impact of fire damage to the entity's servers and equipment. Entities should ensure that server rooms and rooms containing important IT infrastructure are free from clutter and have appropriate fire mitigation measures.

OAG insights and tips

Our observations and recommendations are largely unchanged from previous years. All audited entities received detailed findings and recommendations. All public sector entities must maintain ongoing vigilance and continually enhance their controls to effectively address emerging risks.

1. **To ensure only authorised individuals have access, entities should:**
   a. implement effective access management processes including regular review of user accounts
   b. implement activity monitoring processes to detect malicious activity
   c. strive for passwordless authentication. Where this is not possible, enforce strong passphrases/passwords
   d. implement phishing resistant multi-factor authentication, particularly for privileged accounts
   e. limit and control administrator privileges and system accounts
   f. enforce segregation of duties so that an individual cannot perform the end-to-end process.
2. **To ensure appropriate governance and consistent security, entities should:**
   a. maintain clear information and cyber security policies and roles
   b. classify information and implement data loss prevention controls
   c. conduct regular assessments to ensure the security of their IT supply chain
   d. obtain and review service organisation controls (SOC) type 2 or equivalent assurance reports when they use software-as-a-service (SaaS) applications for key systems including payroll and finance.
3. **To protect workstations, servers and mobile and network devices against cyber threats, entities should:**
   a. promptly identify and address known vulnerabilities
   b. implement data encryption to protect sensitive information from unauthorised access
   c. prevent unapproved applications and macros from executing
   d. enforce minimum security baseline controls for personal or third-party devices
   e. maintain currency of applications and hardware
   f. implement effective controls against malware
   g. implement controls to prevent impersonations and detect/prevent phishing emails.
4. **To reduce the risk of insider threats and unintentional errors, entities should ensure:**
   a. ongoing security awareness training programs are in place and completed by all staff

b. confidentiality/non-disclosure requirements are in place and understood by individuals

c. pre-employment screening is conducted for key positions

d. effective offboarding procedures exist and are followed to ensure timely access cancellation and return of assets.

5. To safeguard networks and critical systems against cyber threats, entities should:

a. prevent unauthorised devices from connecting to their corporate network

b. regularly perform independent penetration tests to verify network security controls

c. segregate their network, particularly for IT and operational technology systems

d. actively monitor network events to allow for effective incident response

e. limit and control administration of network devices.

6. To ensure services, IT systems and information can be recovered in the event of an outage or emergency, entities should:

a. backup critical data to enable recovery after malware, accidental deletion, hardware failure or ransomware

b. maintain up-to-date business continuity, disaster recovery and incident response plans and regularly test them.

7. To deliver and maintain IT services effectively, entities should:

a. have formal service level agreements with suppliers and regularly monitor supplier performance

b. implement policies and procedures to record, review and dispose of assets

c. implement appropriate IT incident and problem management procedures.

8. To ensure existing and emerging IT risks are managed effectively and do not exceed entity risk appetites, entities should:

a. ensure IT, information and cyber security risks are identified, assessed and treated within appropriate timeframes

b. understand their information assets and apply controls based on their value

c. regularly assess controls to ensure they are operating effectively to mitigate risks

d. fully implement their risk management policies to manage IT and cyber security risks.

9. To reduce the likelihood of system outages and service disruptions, entities should:

a. assess and test changes before and after implementation to minimise problems

b. consistently apply change control processes when making changes to their IT systems

c. maintain appropriate change segregation of duties

d. implement controls to detect unauthorised changes.

10. To support the reliability of IT infrastructure and systems, entities should:

a. implement effective physical access controls to prevent unauthorised access

b. ensure the server room is kept suitably clean

c. maintain environmental controls to prevent damage to IT infrastructure arising from heat, moisture, fire and other hazards

d. gain assurance that third-party providers manage data centres appropriately.

In accordance with section 7.12A of the *Local Government Act 1995*, local government entities should prepare a report on any matters identified as significant in the local government's audit report.[7] The report should be given to the Minister for Local Government within three months of the local government receiving the audit report and published on the local government's website.

Resources

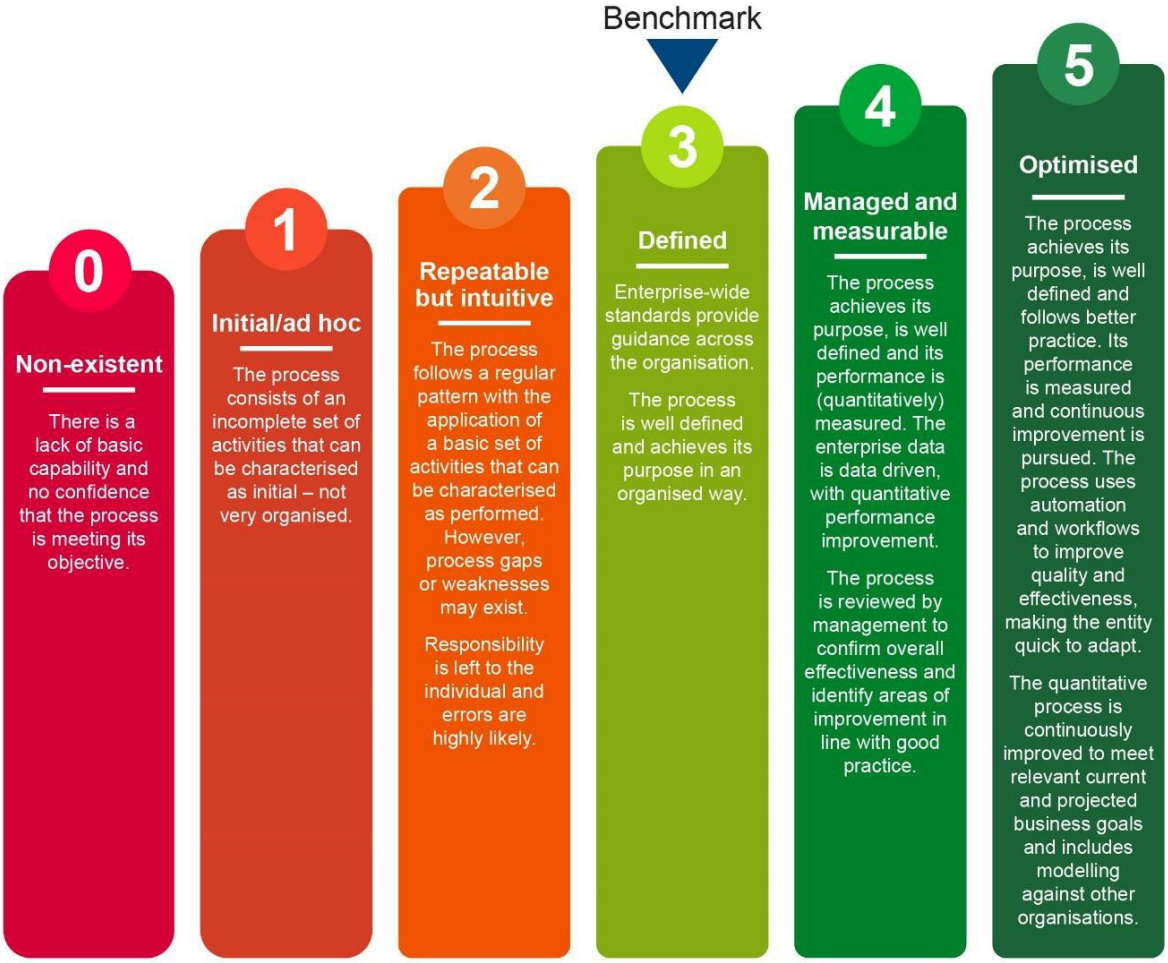
Entities can seek further guidance from various OAG, Office of Digital Government and Australian Cyber Security Centre publications:

- Office of the Auditor General, *Digital Identity and Access Management – Better Practice Guide*, OAG website, 28 March 2024.
- Office of the Auditor General, *Local Government IT Disaster Recovery Planning*, OAG website, 31 May 2024.
- Office of the Auditor General, *Local Government Physical Security of Server Assets*, OAG website, 24 June 2024.
- Office of Digital Government, *WA Government Cyber Security Policy*, WA.gov.au, 1 October 2025.
- Office of Digital Government, *Cyber Security Playbooks*, WA Cyber Security Unit (DGov Technical) website, 5 May 2025.
- Australian Signals Directorate, *Information security manual*, Australian Cyber Security Centre website, n.d.
- Australian Signals Directorate, *Essential Eight explained*, Australian Cyber Security Centre website, 27 November 2023.

The Department of Local Government, Industry Regulation and Safety is collaborating with the Office of Digital Government to deliver a cyber security pilot project to enhance cyber security practices of participating local government entities.

[7] An audit report includes the independent auditor's opinion and the auditor's management report (interim and final management letters) as described in regulation 10 of the Local Government (Audit) Regulations 1996. Further information on what is an audit report is available on our website (https://audit.wa.gov.au/resources/local-government/faqs/#faq-21828).

Appendix 1: Capability assessment benchmark



Source: OAG

Appendix 2: Year-on-year capability assessment result comparison (11 entities in 2024)

These five categories relate to **information and cyber security controls**

Categories	2024	2025*	
Access management	27	9	↓
Endpoint security	18	18	=
Information security framework	36	27	↓
Network security	55	45	↓
Human resource security	55	55	=
Business continuity	45	36	↓
Physical security	64	64	=
Change management	82	64	↓
IT operations	64	64	=
Risk management	100	73	↓

Source: OAG

** Percentages of entities assessed in 2024 that met the benchmark in 2025.*

Auditor General's 2025-26 reports

Number	Title	Date tabled
12	Local Government 2025 – Information Systems Audit Results	25 March 2026
11	Local Government Management of Gifts and Benefits	18 March 2026
10	Controls Over Portable Assets – State Entities	6 March 2026
9	Microsoft 365 Security Controls – State Entities	6 March 2026
8	Status of Local Government Audits 2025	28 January 2026
7	State Government 2025 – Information Systems Audit Results	3 December 2025
6	State Government 2025 – Financial Audit Results	3 December 2025
5	Valuation of Property Held by the Public Education Endowment Trust	3 December 2025
4	WA's Progress to Implement the National Principles for Child Safe Organisations (arising from the Royal Commission into Institutional Responses to Child Sexual Abuse)	27 November 2025
3	Maintaining Regional Local Roads	12 November 2025
2	Gold Corporation – Trade Applications	29 October 2025
1	Management of Housing Maintenance Information	6 August 2025

(Appendix AAR 10.2E)

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

(Appendix AAR: 10.2F)

Office of the Auditor General
Serving the Public Interest

Report 13: 2025-26 | 15 April 2026

FINANCIAL AUDIT RESULTS

Local Government 2025

Office of the Auditor General for Western Australia

Audit team:
Grant Robinson
Kellie Tonich
Tamara McCarthy
Financial Audit teams
Information Systems Audit teams

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.

© 2026 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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/khanhnguyenpictures

(Appendix AAR: 10.2F)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government 2025 – Financial Audit Results

Report 13: 2025-26
15 April 2026

This page is intentionally left blank

(Appendix AAR: 10.2F)

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT 2025 – FINANCIAL AUDIT RESULTS

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

The report summarises the final results of our annual audits of 138 of 147 local government entities for the year ended 30 June 2025.

I wish to acknowledge the assistance provided by the councils, chief executive officers, finance officers and others, including my staff and contract audit firms, throughout the financial audit program and in finalising this report.

Caroline Spencer
Auditor General
15 April 2026

Contents

Auditor General's overview 5

2025 local government reporting cycle at a glance 7

Review of the 2025 financial year 9

What we did 9

Summary of audit opinions 9

Provision of quality financial reports enables timely financial reporting 11

Best practice entities 17

Control weaknesses 18

Improvements in overall control environment 18

Financial management controls 19

Information system controls 23

Improvement opportunities 25

Financial health of local governments 25

Advocacy and reform 27

Governance expectations 28

OAG insights and tips 29

Resources 31

Appendix 1: Status and timeliness of audits 32

Appendix 2: Entities who received an extension from LGIRS to submit their financial report after the 30 September legislated deadline 39

Appendix 3: Qualified and disclaimer of opinions 40

Appendix 4: Prior year qualifications and disclaimers removed in 2025 43

Appendix 5: Emphasis of matter paragraphs included in auditor reports 45

Appendix 6: Delayed 2024 audit material uncertainty related to going concern paragraph 48

Appendix 7: Local government certifications issued since September 2025 49

Appendix 8: Other local government opinions issued since September 2025 50

Appendix 9: Local government current ratios for 2025 51

Appendix 10: Other certifications issued since September 2025 56

Appendix 11: Other opinions issued since September 2025 57

Appendix 12: Opinion and management letter definitions 58

This page is intentionally left blank

Auditor General's overview

This report summarises the results of our annual financial audits of 138 local government entities for the financial year ended 30 June 2025. It also includes results from 11 of the 12 audits outstanding at the time of the *Local Government 2023-24 – Financial Audit Results* report, which have since been finalised.

In 2025, we issued 136 clear audit opinions. Pleasingly, the number of audit qualifications has continued to decrease, with only two of the 138 entities included in this report for 2025 receiving qualified opinions. Of continuing concern is the quality of financial reports submitted for audit. The value of current year errors and the number of prior period errors increased largely as a result of issues linked to property and infrastructure assets. As my office has recommended over successive years, the sector required guidance to support a consistent understanding of valuation obligations and to improve valuation practices generally. So, it is pleasing that the Department of Local Government, Industry Regulation and Safety (LGIRS) recently published this guide on 5 March 2026 which entities can utilise in 2026.

Approximately 33% of entities provided five or more versions of their financial report to my audit teams, with one entity providing 19 versions. As I've said before, this signals a need for greater care and capability in financial reporting. Multiple revisions create delays, cost time and resources and reflect gaps in quality assurance processes. This requires priority attention by entities affected.

This year, for the first time, the online version of this report will include an interactive map graphic to provide insight on our assessment of entity performance from the perspective of financial management control issues raised. This is a useful tool for stakeholders to compare the performance of their local government to those in the surrounding areas or bands. Further, this analysis shows pockets of concerning performance and inability to meet statutory deadlines. We will update this map each year, with the view to showing year on year comparatives.

Of the audits delayed in 2024, four stand out: City of Nedlands, Shire of Coolgardie, Shire of Halls Creek and Shire of Yalgoo. These audits, in conjunction with other delayed audits in 2025 or prior years, were motivating factors behind issuing my recent *Status of Local Government Audits* report[1]. The added public oversight of audit delays is intended to improve timeliness.

This year my team performed some financial health analysis around entities' ability to meet their short-term payment obligations (current ratio) which shows numerous entities facing financial pressure (Appendix 9). Four entities had a ratio of less than one, meaning their current liabilities exceeded their current assets and they may not be able to pay their debts as and when they fall due. The four entities were the: Shire of Coolgardie, Shire of Derby-West Kimberley, Shire of Irwin and Shire of Victoria Plains. The sector-average current ratios continue to decline as do the median ratios. This reflects a sector declining in its ability to meet short-term financial obligations. Our opinion on the Shire of Coolgardie's 30 June 2024 financial report included a material uncertainty related to going concern, indicating that the Shire's ability to continue its financial operations (that is, its financial viability) was not assured. While these concerns were known to my office, they were not publicly disclosed until the Shire's audit report was issued in June 2025. Earlier intervention by councillors and CEOs, and failing that the LGIRS, the Local Government Inspector or the Minister is needed for entities in financial difficulty or crisis.

[1] Office of the Auditor General, *Status of Local Government Audits 2025*, OAG website, 28 January 2026.

It is pleasing to see the sector respond positively to our request to bring audit delivery forward by being audit ready however, there remains opportunities for improvement. The spike in issuing audit opinions (Figure 1) is not sustainable and requires all entities to prepare for earlier completion, thereby enabling more timely reporting to all key stakeholders.

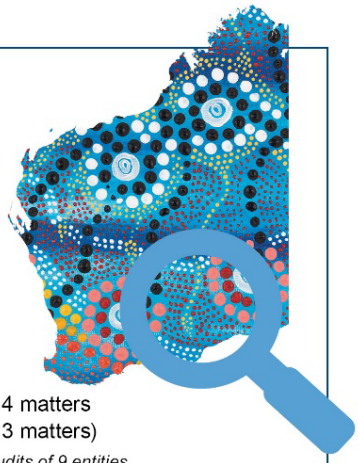
Our advocacy work with entities and LGIRS in relation to legislative reforms has helped reduce certain review requirements for entities, without reducing transparency or accountability. This was a welcome change via the local government legislative reform. It was pleasing to see how responsive LGIRS were to suggestions, and I appreciate their engagement with my office.

Finally, in response to sector feedback, we have refined our best practice entity reporting approach this year. To better reflect the diversity of local government entities, we have aligned our assessment to the WA Local Government banding model[2]. Stakeholders indicated that evaluating best practice at a sector-wide level was less meaningful, and that introducing a level of segmentation would provide clearer and more relevant insights. This change ensures our reporting is more comparable, equitable, and reflective of the unique operating environments within local government. I congratulate those entities recognised as best practice for 2025.

My sincere thanks also to entities, my staff and our contract audit firms for their continued diligent efforts in delivering timely reliable local government financial reports and audits for the Western Australian community.

[2] In Western Australia, local governments are classified into four bands based on the determination of the Salaries and Allowances Tribunal. These bands are used to determine the maximum and minimum number of council members based on the population of the local government district. The classification of local governments into these bands is a key aspect of the *Local Government Act 1995* and is subject to change with new regulations and amendments.

2025 local government reporting cycle at a glance



147 local government entities (PY: 147)

138 audits finalised and the results included in this report (PY: 146)

0* disclaimer opinion (PY: 1)

2* qualified opinions on 4 matters (PY: 10 opinions on 13 matters)

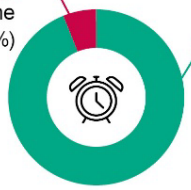
** Does not include the outstanding audits of 9 entities.*

We audited **$5.6 billion** of local government revenue (PY: $5.4 billion)

We audited **$60.7 billion** of total local government sector assets (PY: $59.8 billion)

Timeliness

Audit completion



Audits completed within the prescribed period (by 31 December 2025)

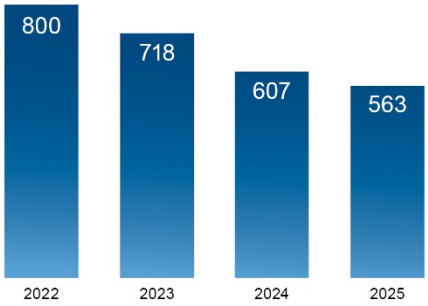
Submission of audit ready financial statement

PY: prior year

Audit results*

** Does not include the outstanding audits of 9 entities.*

Number of financial management issues



0 disclaimer of opinion (PY: 1)

2 qualified opinions (PY: 10)

9 opinions outstanding (PY: 1)

563 financial management issues (PY: 607)

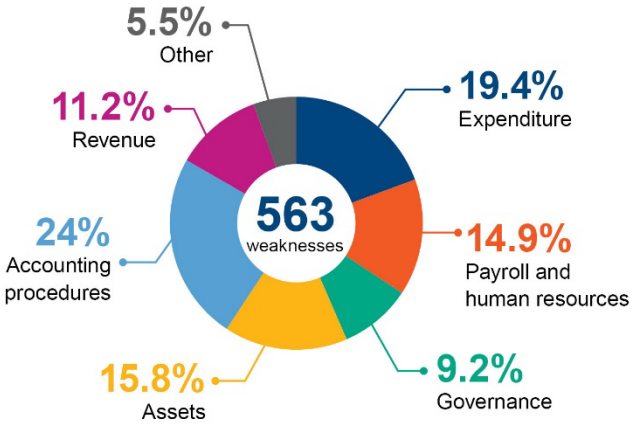
333 information system control issues (PY: 360)

Removed **6** qualified opinions on 7 matters (PY: 6 opinions on 7 matters)

22 emphasis of matter paragraphs (PY: 20)

Financial and management weaknesses

The 138 entities with finalised audits had:



Financial reporting, accountability and audit matters

Quality and timeliness of financial reporting (page 11)

Assets (page 21)

Financial health (page 25)

OAG insights (page 29)

Review of the 2025 financial year

What we did

Our financial audit program is performed under the related Auditing and Assurance Standards Board standards. Our focus is on ensuring the accuracy of an entity's annual financial statements. This report summarises the results of the financial audits of local government entities for the year ended 30 June 2025. It includes the results for 138 of 147[3] entities (Appendix 1), with the remaining nine entities included in our *Status of Local Government Audits 2025* report[4]. Appendix 1 also includes opinion types by local government band to enable entities to compare their own results.

Summary of audit opinions

For the financial year ended 30 June 2025, we issued clear opinions for 136 entities by 31 December 2025, and two audit opinions were qualified. We included 22 emphasis of matter (EoM) paragraphs in the auditor's reports of 22 entities. We also issued 11 audit opinions for entities from previous financial years.

Audit year	2024	2025
Number of entities subject to OAG audit	147	147
Number of entity audits included in results report	135	138
Number of entity audits included in updated statistics	146	N/A
Clear (unqualified) audit opinions	135	136
Qualified opinions	10	2
Disclaimer of opinion	1	0
Material uncertainty related to going concern	2	0
Emphasis of matter paragraphs	20	22

Source: OAG

Table 1: Audit results for the past two years

Entities that did not make the 2024 results report cut-off included in this report

At the cut-off date of this report, with the exception of the Shire of Yalgoo, all entities outstanding in the *Local Government 2023-24 – Financial Audit Results* report have now been finalised. While many of these entities received clear 2024 audit opinions, this may not have been the case had the audits been completed on time. The delays with these audits were mostly to give entities time to provide more evidence and correct their financial report. Delays in audits present significant inefficiencies, cost impacts and resourcing pressures on audit teams.

Disclaimer removals

Following a disclaimer of opinion, we generally qualify the comparability of the current year's financial results with the prior year, as the prior year figures were not audited and may be incorrect. Further, when an entity restates figures from a disclaimer year, and they cannot be

[3] 31 December 2025 is the statutory deadline for local government entities to complete their audits and is used as the statistics cut-off date for this report.

[4] Office of the Auditor General, *Status of Local Government Audits 2025*, OAG website, 28 January 2026.

audited, another related qualification is issued. These qualifications alert users to exercise care when comparing the two years.

The 2024 audit reports for the City of Nedlands and Shire of Halls Creek (issued during 2025) featured disclaimer removals, as did the Shire of Toodyay's 2025 audit report.

The City of Nedlands 2024 audit report contained one qualification on comparability as the prior year numbers could not be audited.

The Shire of Halls Creek 2024 audit report contained three qualifications:

- one was on comparability as the prior year restated numbers could not be audited
- a related qualification, the current year disclosure note on the restated numbers could not be audited
- a third qualification for not valuing other infrastructure assets at 30 June 2022 or 2023.

The Shire of Toodyay 2025 audit report contained three qualifications:

- two were as per the Shire of Halls Creek, comparability of restated numbers which could not be audited, and the related disclosure note
- a third qualification was for unreconciled amounts in cash and cash equivalents.

Full details of the qualifications issued for these three entities can be seen in Appendix 4.

Two qualified opinions

The Shire of Boyup Brook and the Shire of Toodyay were the only entities to receive qualified audit opinions in 2025. This represents a decrease compared to 2024, which recorded 10 entities with audit qualifications out of 146 completed audits. We expect there will be more audit qualifications to come from the nine entities that did not meet their statutory deadline.

The two qualified entities in 2025 had four qualification matter paragraphs, two of which relate to prior year disclaimed opinions (refer above: disclaimer removals). The audit qualifications are included in Appendix 4.

Emphasis of matter paragraphs (EoM)

In 2025, we included 22 EoM (Appendix 5) paragraphs in 22 entity audit reports which is relatively on par with the 20 EoM paragraphs included in 20 reports the prior year. We expect the number of EoM's to increase as the outstanding nine audits are finalised. This year EoM paragraphs directed the readers' attention to:

- restatements of comparative figures or balances to correct prior period errors, largely related to property and infrastructure assets (2025: 16 entities) (2024: 16 entities)
- the basis of accounting used by the entity (2025: 2 entities) (2024: 1 entity)
- investment in associates (2025: 4 entities) (2024: 0).

This year we refined our use of EoM paragraphs relating to prior period errors. Auditing standards allow judgement in this area. We now only include an EoM where errors are deemed fundamental to users' understanding of the financial report. This ensures EoMs highlight to users what is essential for their consideration. While the number of EoM paragraphs this year is similar to 2024, all 2025 errors were serious enough to impact users' understanding of the financial report. This is more concerning, especially as the number would have been higher without our refined EoM approach.

We have a section of this report dedicated to prior period errors, refer to the prior period errors section. A full description of EoM paragraphs is included in Appendix 5.

Material uncertainty related to going concern

Under Australian Auditing Standards, we consider whether events or conditions exist that may cast significant doubt on the entity's ability to continue as a going concern. Essentially, if an entity can fund their continuing operations, they are considered to be able to continue as a going concern.

This applied to the Shire of Coolgardie's 30 June 2024 financial position. This audit was not finalised until June 2025 and therefore it was not included in our *Local Government 2023-24 – Financial Audit Results* report[5]. The audit had challenges largely stemming from the Shire's financial situation and resourcing issues.

The material uncertainty related to the Shire's ability to continue as a going concern, as it had incurred a net loss of $4.6 million for the year ended 30 June 2024. At that date, the Shire's current liabilities exceeded its current assets by $14.2 million and the unrestricted cash balance was overdrawn by $934,000. The Shire disclosed these details along with options available to them to navigate their way through these challenges in a note to the financial statements.

The Shire's 30 June 2025 audit report did not include a material uncertainty related to going concern. A case study of the Shire's financial health is included in the section on financial health of local governments.

Provision of quality financial reports enables timely financial reporting

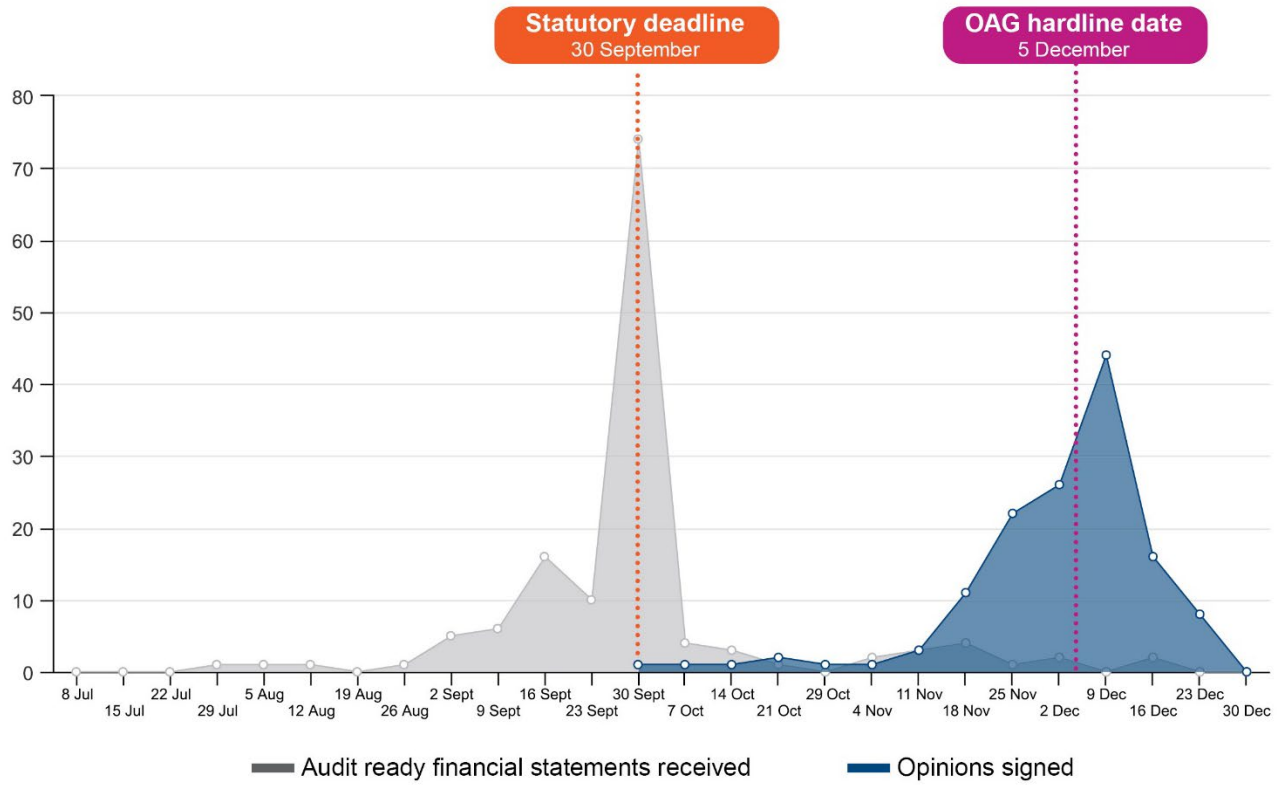
Provision of financial reports

While 84% of the 138 local government entities included within this report provided their financial report by the legislated deadline of 30 September 2025, 54% of entities provided their financial report during the week of the deadline. One-third of entities provided their financial report to the auditors on the deadline. This can be seen in the clear spikes in Figure 1 which suggests entities may be aiming for legislative compliance rather than better practice. Similarly, there is a peak in the number of audit opinions issued at the date of our hardline initiative[6], on 5 December for 2025. In the week ended 5 December 2025 we issued approximately a third of the 138 opinions included in this report. Again, this represents compliance rather than better practice. To encourage sector-wide uplift and a culture focused on improvement, we encourage entities to access our suite of better practice and audit readiness tools to assist them in earlier financial reporting.

An audit-ready financial report is the starting point for a financial audit, without this, auditors are unable to commence their work in earnest. Also of concern is the accuracy of the financial reports provided. Only 6% of entities required no adjustments to their financial report. The remaining entities needed to make adjustments to their financial report, indicating a lack of quality. Further details on audit adjustments are included in the quality section of this report.

[5] Office of the Auditor General, *Local Government 2023-24 Financial - Audit Results* , OAG website, 24 April 2025.

[6] Our hardline initiative is focused on improving the quality and timeliness of financial reports and associated workings provided for audit. As part of the approach, we will no longer wait until the entity is ready if key information and people are not reasonably available within the agreed schedule. Instead, we will issue our audit opinion on the information available, even if this results in a qualified audit opinion.



Source: OAG

Figure 1: Financial reports received and audit completion dates by week

Timeliness of reporting

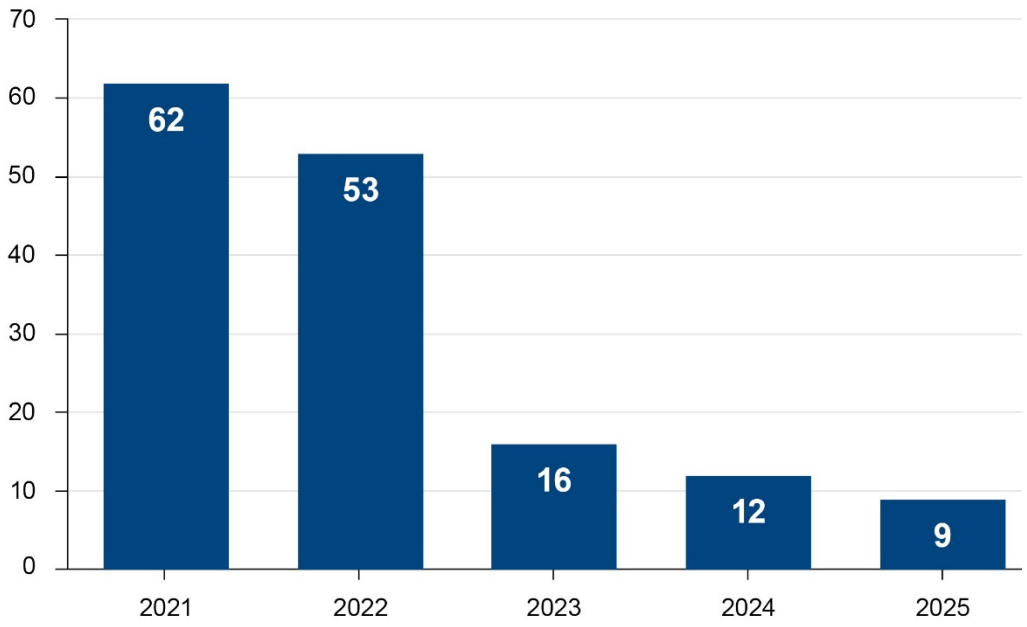
More opinions meeting statutory deadlines

For the first time, we issued a standalone report on the timeliness of local government audit opinions[7]. This new reporting initiative increases transparency, to Parliament and the community, on entity financial report progress and reinforces our commitment to issuing all audit opinions by 31 December, in line with legislated timeframes.

In 2025, 94% of local government audit opinions were issued by the statutory deadline, a continued improvement on prior years. We anticipate further improvement in 2026, with the long-term aim that all audits are completed well within the required timeframe.

Since 2023, we have provided entities with an early December target date, previously referred to as the OAG hardline initiative, to support earlier audit completion and reduce the risk that minor delays push audits beyond 31 December. For the 2025 cycle, this date was 5 December. This initiative has contributed to a significant reduction in the number of audits outstanding at 31 December, as shown in Figure 2.

[7] Office of the Auditor General, *Status of Local Government Audits 2025*, OAG website, 28 January 2026.



Source: OAG

Figure 2: Number of audits outstanding at 31 December for the last five years

For the nine outstanding audits included in the *Status of Local Government Audits 2025*[8] report in January 2026, the only substantive change is for the Shire of Yalgoo with their 2023 and 2024 audits now finalised, and the Shire of Dalwallinu with their 2025 audit now finalised. For both 2023 and 2024 the Shire of Yalgoo's audit opinions were qualified in respect of:

- bank reconciliation issues
- accrued income recoverability
- valuation of infrastructure asset (roads) not being undertaken.

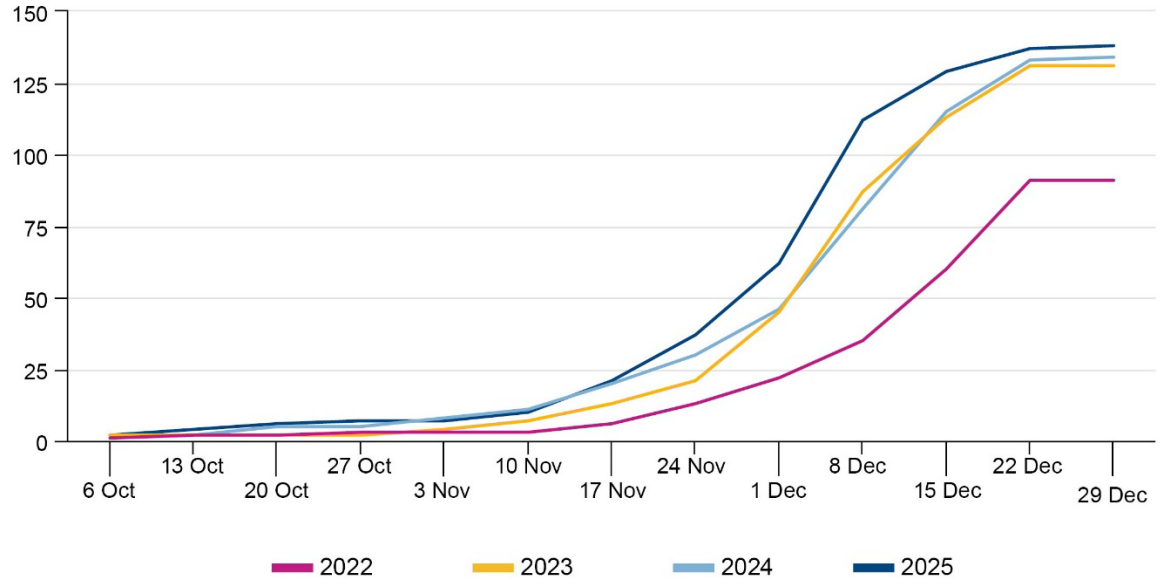
Despite delayed lodgements in 2024 the following entities, through appropriate commitment and resolve, successfully addressed the contributing issues and met the statutory deadline in 2025:

- City of Greater Geraldton
- Shire of Bridgetown-Greenbushes
- Shire of Collie
- Shire of Coolgardie
- Shire of Dundas
- Shire of Nannup
- Shire of Toodyay (last met the statutory deadline in the 2020 financial year)
- Shire of Wickepin
- Town of Cottesloe.

[8] Office of the Auditor General, *Status of Local Government Audits 2025*, OAG website, 28 January 2026.

Overall Progress is positive, but audit bottleneck continues

Figure 3 shows that 2025 was ahead of previous years in terms of number and timing of opinions issued. While the improvement in timeliness is encouraging, there continues to be a bottleneck of audit opinions being issued in December.

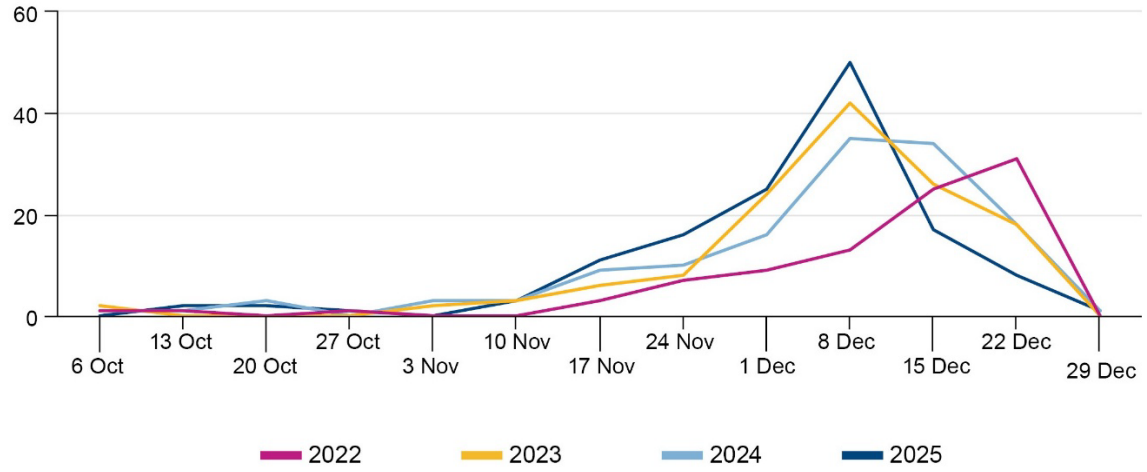


Source: OAG

Figure 3: Cumulative opinions issued from October to December for 2022 to 2025

We are pleased with the sector successfully responding to our efforts to bring audit delivery forward before the 31 December deadline, although there remain opportunities for improvement. There is concern that entities treat our hardline initiative date as their target for receiving an opinion. There were 58% of 2025 local government opinions issued in December, with 33% of opinions issued during the week ended 5 December 2025. The clear spike in opinions issued around this date is shown in Figure 4.

This spike in issuing opinions is unsustainable. Looking forward we want to see entities preparing for earlier audit completions to create a smoother curve of opinions being issued, rather than a sharp spike. This would enable earlier reporting by entities to their ratepayers and have the added benefit of reducing the pressure on finance teams and auditors.



Source: OAG

Figure 4: Opinions issued per week 2022 to 2025

Quality

Good quality financial reports are accurate, clear and complete.

Errors and the number of versions of the financial report submitted to audit are indicators of the quality of financial operations of an entity. Both are indicative of a weakness in an entity's financial report preparation process. It creates additional effort, both internally for the entity and for the auditor, which leads to increased costs (internally and audit fees).

Prior period errors are increasing

A prior period error is a significant misstatement or omission, made by an entity in previous financial years, identified during the current year. It is usually corrected retrospectively by restating the opening balances in the financial statements. Entities with prior period errors have increased by 13% from 2024, with the 2025 numbers subject to increase as the nine outstanding audits are finalised. Many errors relate to asset accounting.

Common themes were:

- found assets
- valuation errors
- duplicate assets.

The growth in prior period errors and continued presence of asset related errors demonstrates a need for entities to focus on improving their asset accounting processes. As revaluations are only required every five years, many entities are in the outer year of a valuation cycle. We expect these errors could get worse in a valuation year.

A compounding issue with prior period errors, once identified, is that many entities are unsure how to correctly account for and disclose these errors in their financial reports. This contributes to inconsistent treatment across the sector and increases the level of auditor involvement required to resolve the matters.

Financial report versions still too high

On average we received four versions of an entity's financial report in 2025, similar to 2024. While the proportion of entities with only one version of the financial report prior to finalisation has increased to 6% (3% in 2024), this proportion is insufficient.

Approximately 33% of entities provided five or more versions of their financial report to audit, which is consistent with the previous year. We consider five or more versions of a financial report to be excessive, and indicative of a lack of financial management and reporting expertise and audit readiness by entities. One entity was a concern with 19 versions of their financial report provided to audit. This is an increase from 2024 where one entity had 16 versions for their financial report before finalisation.

Each version of the financial report provided to auditors needs to be reviewed, compared to previous versions with changes being queried and validated. All of which increase audit hours and costs. Entities should be aiming for one to two versions of their financial report. Any more than this indicates inadequate quality review processes in the preparation of the report.

Value of errors increase in 2025

The number and value of adjustment errors made to financial statements increased in 2025.

Errors are identified during the audit process, and we advise entities of those that are more than clearly trivial. Material errors must be corrected to avoid a potential modified opinion,

while immaterial errors may be left unadjusted where they do not affect the fair presentation of the financial report.

Year	Adjusted errors			Unadjusted errors			Total errors	
	No. of entities	No. of errors	Value	No. of entities	No. of errors	Value	No. of errors	Value
2025	98	301	$674,314,611	55	125	$43,987,252	426	$718,301,863
2024[9]	100	297	$393,532,137	63	137	$58,713,391	434	$452,245,528
2023	100	285	$1,125,288,333	59	104	$69,157,705	389	$1,194,446,038
2022	91	335	$1,613,529,048	58	132	$50,668,884	467	$1,664,197,932

Source: OAG

Table 2: Adjusted and unadjusted errors for entities

Entities should exercise discretion when considering adjustments for immaterial errors. While these smaller errors may not affect the fair presentation of the financial report, processing and validating them consumes time and resources.

Entities need to strike a balance between the overall objective of presenting a fair financial report and the additional effort required to process adjustments. Each adjustment not only increases the entity's workload but also requires auditors to perform further validation and review additional versions of the financial report, increasing audit time and cost, and resulting in delay for both parties.

While the overall number of errors for 2025 appears relatively consistent with 2024, we expect this to increase once the nine outstanding audits are finalised.

The Shire of Toodyay and Town of Claremont had the equal largest number of adjusted errors in 2025, with 10 errors each. The Shire of Toodyay adjusted errors amounting to $10.3 million, whilst the Town of Claremont's adjustments amounted to $38.9 million. Two other entities were significant outliers due to the value of their adjustments:

- The City of Albany undertook infrastructure valuations (internally) for the 2025 financial year that indicated an increase in value of infrastructure assets of $148 million, which was recorded. However, the valuation was unable to be relied upon for audit purposes as it lacked sufficient supporting evidence. Accordingly, the revaluation adjustment was subsequently reversed.
- The City of Swan recorded $75.6 million across two adjustments to correct their works in progress (WIP) balance as disclosed in the note:
    - $18.5 million of property, plant and equipment (PPE) additions were incorrectly classified as transfers from WIP
    - $57.1 million in infrastructure additions were incorrectly classified as transfers from WIP.

  These changes only relate to the WIP balance and PPE disclosures and were not impacting the overall PPE balance in the statement of financial position.

These outliers contributed to the overall increase in value of errors; however, the uplift in error values is evident across the sector.

[9] 2024 numbers have been restated and are now inclusive of 11 entities which have been signed out since our *Local Government 2023-24 Financial Audit Results* report.

Best practice entities

This year we are reporting best practice entities in two categories:

- top 10 band 1 and 2 entities
- top 20 band 3 and 4 entities and regional councils.

This is a change from our prior reporting of a top 20 of all entities. The change better reflects differences, complexities and numbers of entities within the various bands. The number of entities in bands one and two makes up 30% of the total 147 local government entities. Bands three, four and regional councils make up the remaining 70%.

The criteria we rate entities on remains unchanged. We rate entities on their financial reporting practices against the following criteria:

- timeliness of CEO-certified financial report
- quality of financial report (including the number of errors identified)
- quality of working papers that support the financial report
- management resolution of accounting matters
- key staff availability during the audit
- number and significance of management letter findings
- clear opinion with no EoM or other audit report modifications.

We congratulate the entities we rated as the top achievers for 2025.

Best practice top entities	
Top 10 Band 1 & 2	**Top 20 Band 3, 4 and other entities**
• City of Belmont • City of Cockburn • City of Fremantle • City of Greater Geraldton • City of Rockingham • City of Vincent* • Shire of Mundaring* • Shire of Murray* • Shire of Northam • Shire of Wyndham-East Kimberley	• Murchison regional vermin council • Shire of Beverley* • Shire of Boddington • Shire of Chittering • Shire of Christmas Island* • Shire of Donnybrook-Balingup • Shire of Exmouth* • Shire of Gingin • Shire of Irwin* • Shire of Lake Grace* • Shire of Laverton • Shire of Menzies* • Shire of Nannup • Shire of Narembeen • Shire of Ngaanyatjarraku • Shire of Peppermint Grove • Shire of Three Springs* • Shire of Wagin • Shire of Waroona • Shire of Wyalkatchem

Source: OAG

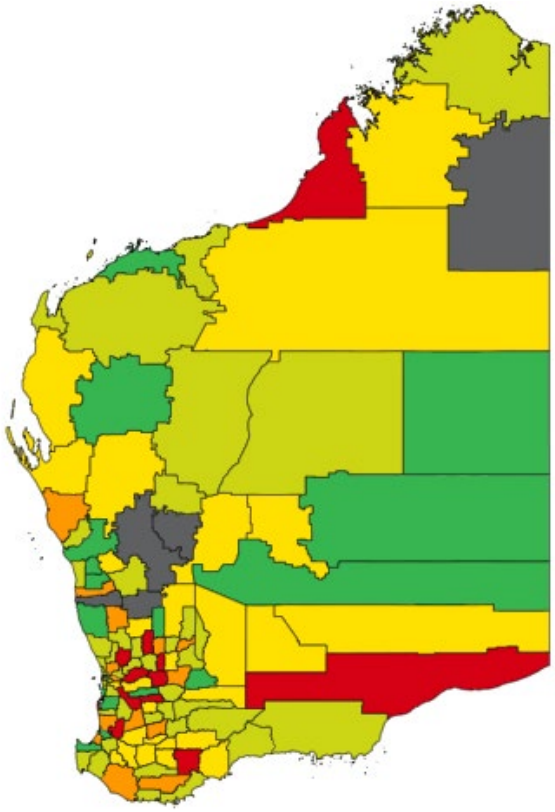
** Indicates entities which received best practice in the Local Government 2023-24 – Financial Audit Results report.*

Table 3: Best practice entities for 2025

Control weaknesses

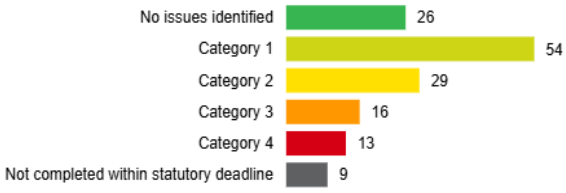
Improvements in overall control environment

An entity's control environment includes the governance and management functions as well as the attitudes, awareness and day-to-day actions that contribute to the internal control practices of importance to the entity. We reported a total of 896 control findings in 2025 which is a decrease from the prior year (967 control findings). These are made up of 563 financial management issues (2024: 607) and 333 information systems (IS) control issues (2024: 360).



For the first time in 2025 we have compiled an interactive map graphic to provide clear visuals on the comparative financial control performance of local governments. Figure 5 is only accessible via the online version of this report. This graphic can be filtered by WALGA region, local government band or metro or regional entities.

This is a useful tool for stakeholders to compare the performance of their local government to those in the surrounding areas. Further, this shows pockets of concerning performance and inability to meet statutory deadlines. We will update this map each year, with the view to showing year on year comparatives.



Source: OAG

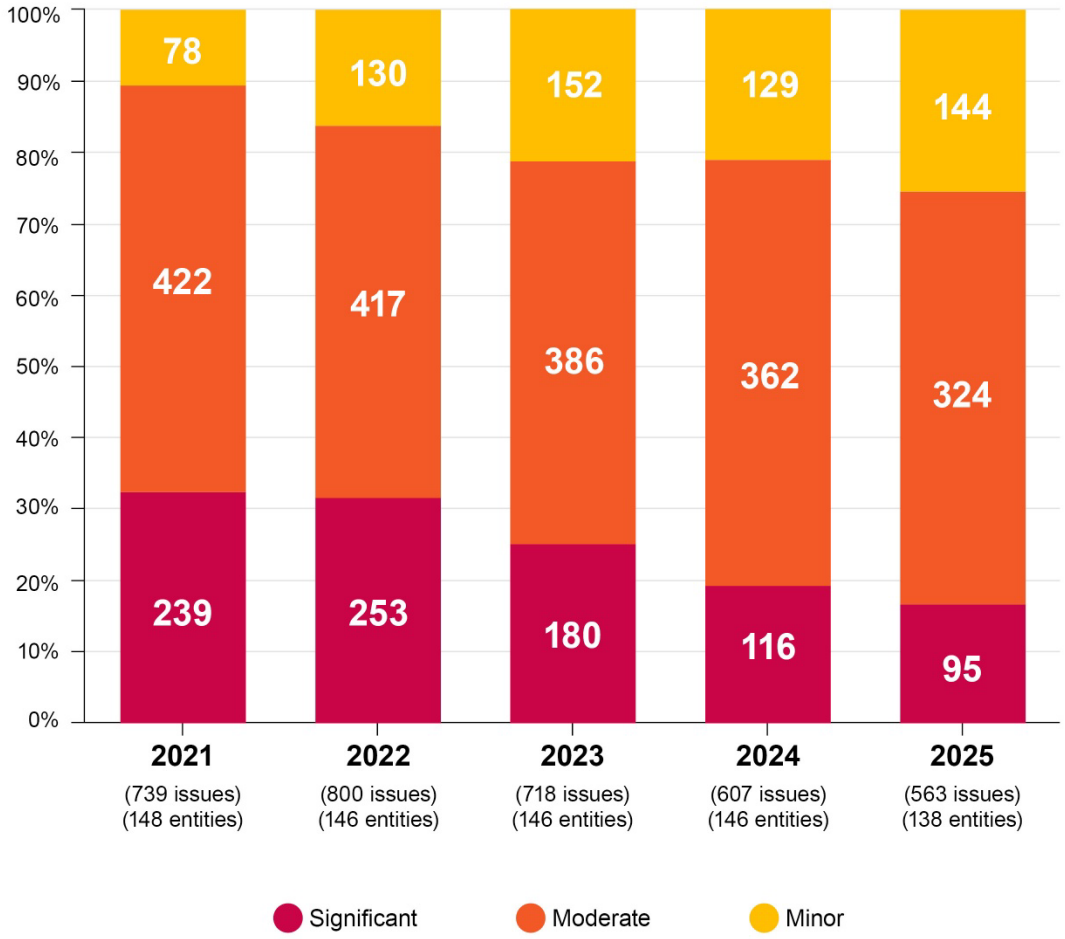
Figure 5: Entities by financial management control rating category

Our audits are primarily focused on controls that support the preparation of the financial report. A control environment with adequate systems, processes and people reduces the risk of error and fraud, and provides assurance to management, council and other stakeholders that financial reports are materially correct. We assess each entity's control environment during our risk assessment procedures. We report details of weaknesses identified through the audit process in the control environment to entities management and those charged with governance. The main themes of these weaknesses are discussed in further detail. We reported in detail the IS control findings in a separate report to Parliament.[10]

[10] Office of the Auditor General, *Local Government 2025 – Information Systems Audit Results report*, OAG website, 25 March 2026.

Financial management controls

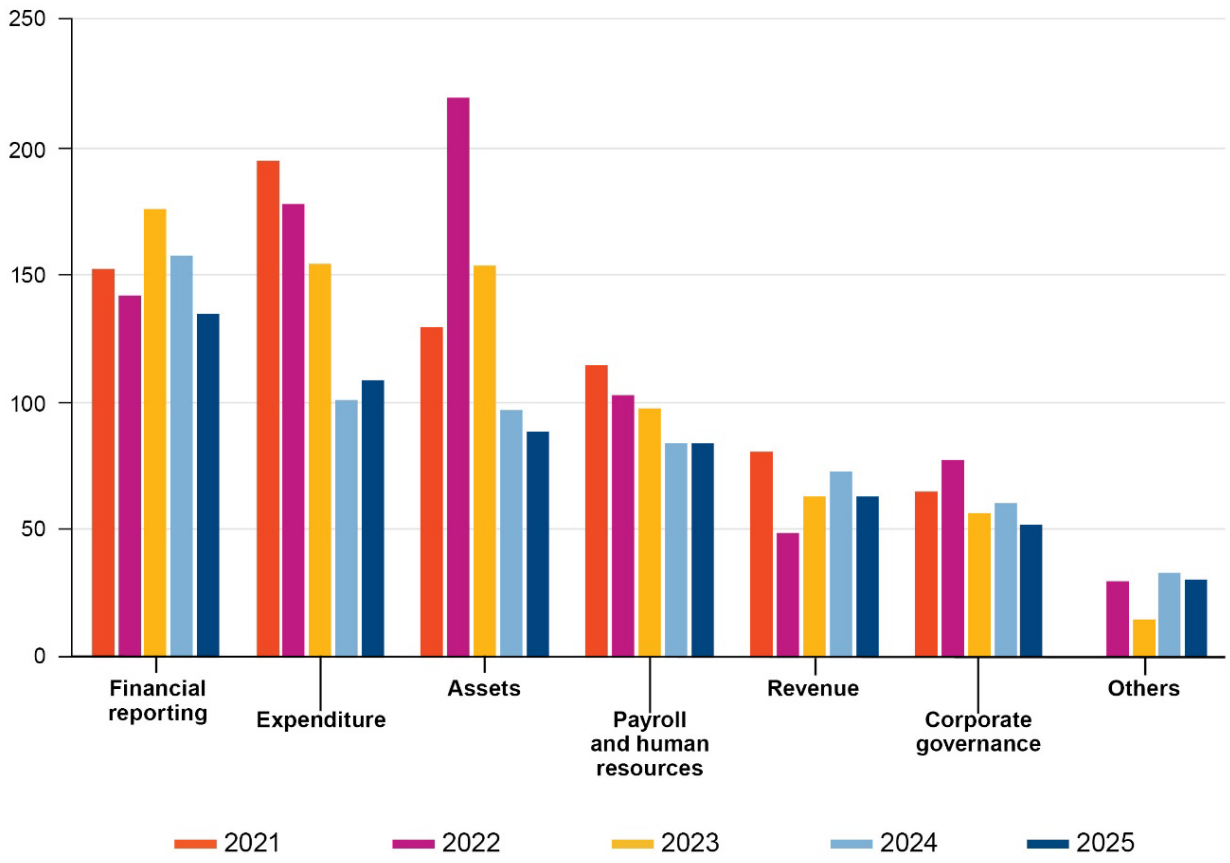
In 2025, management letter issues continued their downward trend, reducing from 607 in 2024 to 563. The number of entities with reported control weaknesses also decreased, from 130 in 2024 to 112 in 2025. The number of control weaknesses is expected to increase once the nine outstanding audits are finalised. The reduction was driven by fewer significant and moderate findings, though minor issues increased in both number and proportion as can be seen in Figure 6. Definitions of our finding risk ratings are included in Appendix 12.



Source: OAG

Figure 6: Proportion of control weaknesses reported to management in each rating category

The movement in findings by category was mixed for 2025, as seen in Figure 7. Financial reporting remained the largest area of concern, although the number of issues decreased slightly compared to 2024. Conversely, issues relating to expenditure increased modestly year on year. Other categories either decreased slightly or remained broadly consistent with 2024.



Source: OAG

Figure 7: Financial management control issues reported to entities by category

Financial reporting

We raised 135 issues (2024: 158 issues) across 70 entities (2024: 77 entities) relating to their financial reporting procedures. Of these issues, 49 were unresolved from the prior year and 14 were rated as significant.

- **Journal entries and reconciliations:** 27% of issues (36 issues) related to journal entries and general ledger reconciliations (excluding bank reconciliations). Journal entries are commonplace but present a high-risk area, as they adjust approved transactions. Key controls include appropriate review processes and segregation of duties between those who post and those who approve journals. Without these controls, the risk of error and fraud increases. Similarly, when finance system balances are not reconciled to sub-systems in a timely manner, errors within the financial report are more likely. These risks are further compounded when reconciliations are not appropriately reviewed. Importantly, these control weaknesses are readily addressed through the implementation of basic controls.

- **Policies and procedures:** 22% of issues (30 issues) related to policies and procedures, predominantly where they were outdated, not recently reviewed, or not implemented. Without up-to-date approved policies and procedures, staff may be unaware of council and management expectations regarding their responsibilities and the performance of key transactions and activities. This increases the risk of errors, fraud and non-compliance.

- **Bank reconciliations:** 16% of issues (22 issues) related to bank reconciliations. Bank reconciliations are a critical financial management control for all entities. As with

general ledger reconciliations, inadequate reconciliation processes increase the risk of errors and undetected fraud. This risk is heightened for bank reconciliations due to their direct connection to cash balances, which are more susceptible to misappropriation if controls are weak. We again found instances of basic reconciliations not being performed or reviewed in a timely manner, and reconciling items remaining long outstanding.

Preparation of an accurate financial report requires timely completion of reconciliations and high quality supporting working papers. These should be provided to auditors at the commencement of the audit. We expect the financial report to be reviewed by the CEO and council or the audit committee prior to submission, ensuring its completeness and accuracy. Following this review, the CEO should sign the financial report and submit it for audit. Guidance for entities is available in our better practice guides, accessible on our website[11].

Expenditure

We reported 109 expenditure weaknesses to 61 entities in 2025, compared with 101 issues to 64 entities in 2024. Of these 109 weaknesses, 33 were unresolved from the prior year and five were rated as significant. Poor procurement practices continue to be of concern, as they increase the risk of fraud and reduce the likelihood that entities achieve value for money. Entities need to ensure they have appropriate controls and processes in place that operate effectively to mitigate these risks.

- **Purchase orders:** As with previous years, we identified instances where purchase orders were raised after the invoice date and where entities did not seek an adequate number of quotes. Obtaining an appropriate number of quotes is an important control to ensure value for money. Purchases made without authorised purchase orders increase the risk of unauthorised spending. These issues accounted for 52% (57 issues) of all expenditure related findings.
- **Supplier master files:** Issues relating to supplier master files formed the second largest category of expenditure findings, representing 17% (19 issues). Strong controls over supplier master files are essential in preventing fraudulent payments. Where controls are weak, there is an increased risk that payments may be made to incorrect or fraudulent bank accounts.
- **Credit cards:** Credit card controls accounted for 16% (17 issues) of findings. We identified instances where credit card purchases were not supported by receipts, transactions were not appropriately reviewed or approved, and credit card policies were not complied with. This reflects non-compliance with policies and procedures and increases the risk of fraud.

Asset management

We identified 89 findings at 56 entities in 2025, compared with 97 findings at 57 entities in 2024. Of the 89 findings, 27 were prior year issues which remained unresolved, and eight were rated as significant.

- **Valuations:** Most asset management findings related to valuations, comprising 26% of issues (23 issues). This area was a key source of findings in 2023 but not in 2024. This fluctuation is partly due to the cyclical nature of valuations under local government regulations, which require entities to revalue assets every five years. Each year a different cohort of entities is due for revaluation, influencing the number and nature of findings identified.

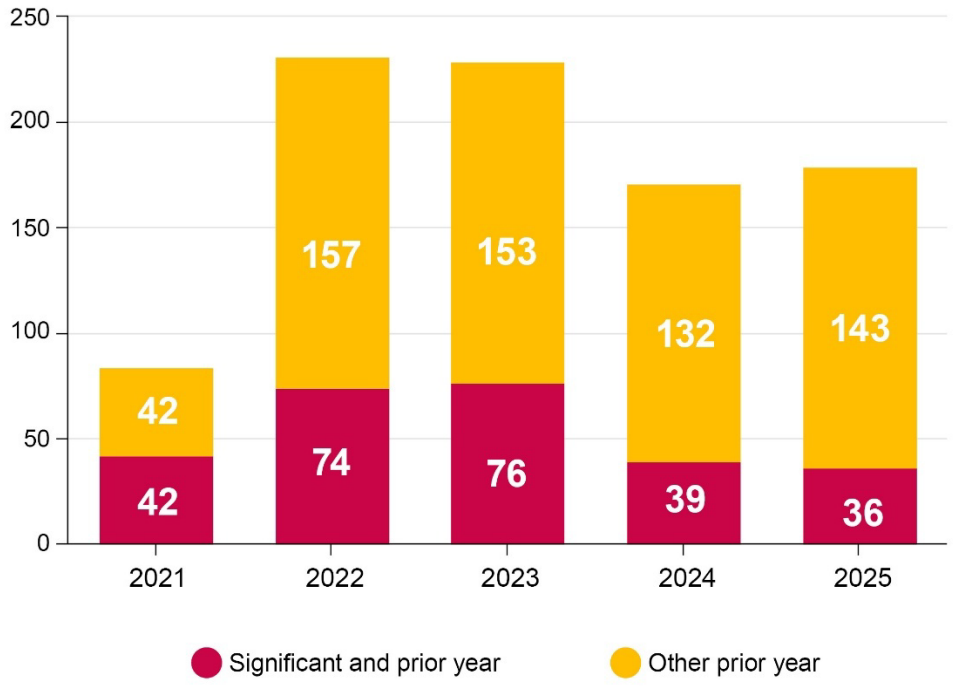
[11] Office of the Auditor General, *Better practice guidance*, OAG website, n.d., accessed 9 February 2026.

- **Capitalisation of works in progress (WIP):** The second largest category of asset management findings related to WIP, representing 20% (18 issues) in 2025. These findings generally related to late capitalisation of WIP, where assets were available for use or already in use, but were not depreciated. In some cases, errors involved assets from prior years that should have been transferred from WIP but were not, resulting in prior period errors.
- **Asset reconciliations:** Asset reconciliations were the third largest category, comprising 18% (16 issues). Reconciliations ensure that asset records are complete, accurate and aligned between the finance and asset systems. Where reconciliation processes are inadequate, entities risk losing track of assets or incorrectly recognising them, which can affect asset valuations and lead to found asset errors in future years.

Control weaknesses in asset management can lead to qualified audit opinions due to the material value of property and infrastructure assets held by local governments. Entities need to remain vigilant and ensure valuation, capitalisation and reconciliation processes are robust and consistently applied each year.

Findings unresolved from prior year

For 2025, 179 financial management control findings raised across 81 entities (2024: 171 findings across 77 entities) remained unresolved from prior years. This represents 32% of all current year findings (2024: 28%). Of these unresolved issues, 20% (36 issues) (2024: 23% 39 issues) were rated as significant, requiring urgent action. While the proportion of significant unresolved findings has remained consistent, it is concerning that the number of unresolved issues increased.



Source: OAG

Figure 8: Prior year issues per year

Unresolved findings from prior years primarily relate to financial reporting, expenditure and asset management. These unresolved issues align with the underlying themes previously identified within this report, for each category. It is concerning that these matters remain

unresolved, as they continue to add to audit time and costs. Entities need to prioritise addressing these issues, particularly those rated as significant.

Information system controls

The purpose of general computer control (GCC) audits is to assess the effectiveness of entities' computer controls relied on to accurately process and maintain the integrity, confidentiality and availability of key financial business systems and information.

For the 2025 financial year, we reported 333 general computer control weaknesses to 68 entities, compared to 360 control findings to 89 entities in 2024. Over half of these weaknesses (60%) were unaddressed prior year issues. Nine percent of findings were rated significant, 69% moderate and 22% minor (Figure 9).

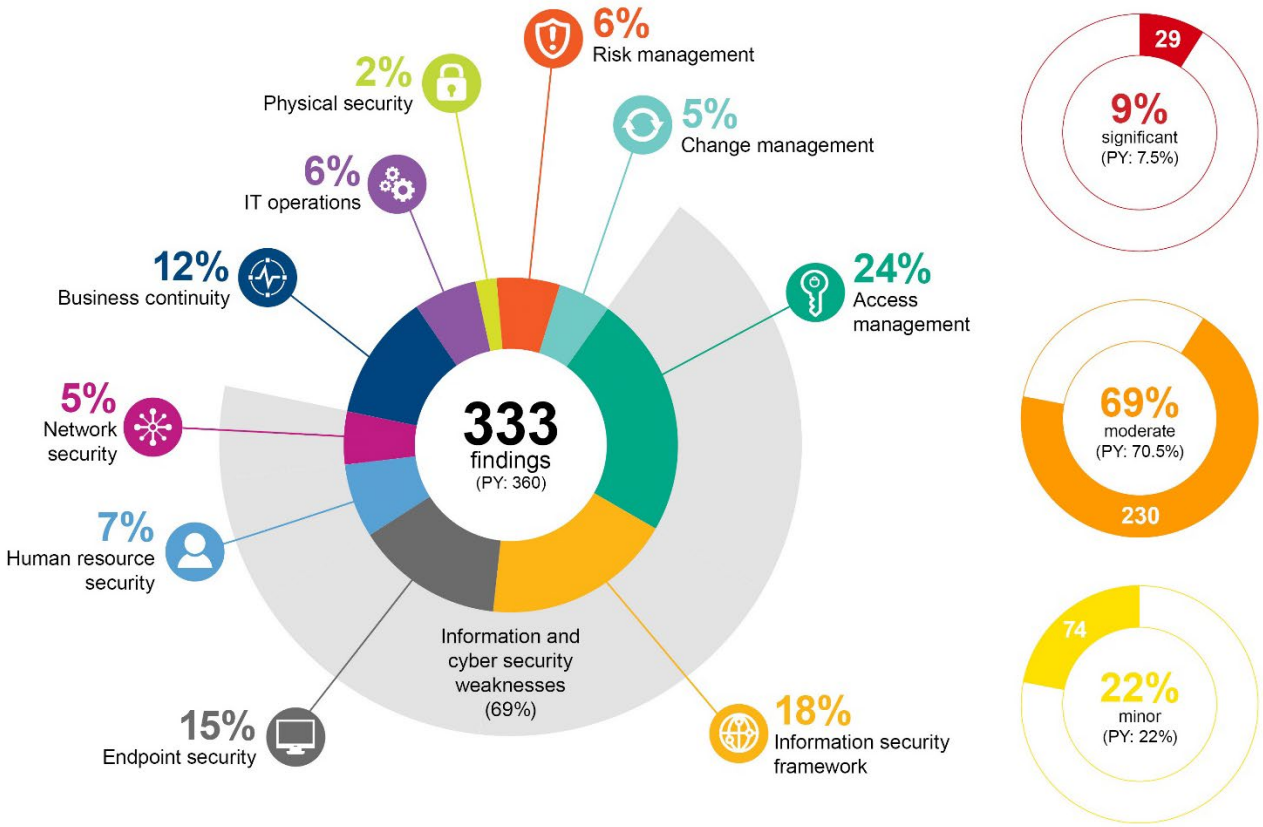
Entity controls in the following control categories showed significant weaknesses:

- access management
- business continuity
- endpoint security
- information security framework
- network security.

Of the 333 weaknesses identified, the majority related to information and cyber security controls:

- 24% related to managing access, such as delays in removing access of former staff and contractors, poor control over privileged and system accounts, and insufficient user activity monitoring.
- 18% related to information security framework weaknesses. These issues comprised insufficient information and cybersecurity policies, as well as governance and compliance weaknesses.
- 15% related to controls to protect endpoints (end user devices and servers). These included system vulnerabilities, legacy systems, and limited controls to prevent malware.

The *Local Government 2025 – Information Systems Audit Results* report presents a detailed analysis of these findings.



Source: OAG

Figure 9: Information system weaknesses across 10 control risk categories and ratings

Improvement opportunities

Financial health of local governments

Financial sustainability is a challenge for many local governments across the country due to a combination of:

- operating losses
- declining cash reserves
- increasing compliance and complexity
- limited capacity to generate sufficient own source revenue (from existing or alternative means)
- the general economic environment.

These factors are just as relevant in Western Australia and were most evident for the Shire of Coolgardie in 2024 when we included a material uncertainty related to going concern in the Shire's 2024 audit report.

Case study 1: Historical financial viability concerns at the Shire of Coolgardie

Under the going concern basis of accounting, financial statements are prepared on the assumption that an entity will continue operating for the foreseeable future. Auditors are required to report when there is a material uncertainty about an entity's ability to continue as a going concern.

For the Shire of Coolgardie's 2024 audit, finalised on 23 June 2025, we highlighted concerns by drawing attention to note 1 of the Shire's financial report. The note disclosed that the Shire:

- recorded a net loss of $4.6 million for the year ended 30 June 2024
- had current liabilities exceeding current assets by $14.2 million
- had an overdrawn unrestricted cash balance of $934,000
- had inappropriately used restricted funds for operational purposes.

These issues, along with other disclosures in the financial report, indicated the presence of a material uncertainty that cast significant doubt on the Shire's ability to continue as a going concern.

Following the 2024 audit, the Shire undertook debt restructuring and other initiatives to improve its financial position. We were satisfied with these actions, and as a result, a material uncertainty paragraph was not required in the 2025 audit report. However, because the 2024 audit report and financial statements were the first public signal of concerns, the situation highlights the importance of stronger monitoring and guidance for entities on financial sustainability.

LGIRS has developed the Local Government Financial Indicator (LGFI) tool, which provides a point-in-time assessment of an entity's capacity to meet its short and long term financial obligations, having regard to its funding sources. The LGFI replaced the former Financial Health Indicator (FHI) and, unlike the FHI, is not designed to assess longer term

financial sustainability. Further information on the methodology and application of the LGFI is available through the MyCouncil FAQs[12].

LGFI data was first published on the MyCouncil website in May 2025 for the 2019 to 2023 financial years. As the indicator relies on audited financial information, data publication necessarily follows the completion of audit and associated validation processes. At 23 February 2026, LGFI results were available up to the 2023 reporting period, with subsequent years to be released in line with established update schedules. However, the indicator is only genuinely useful when it is updated in a timely manner after audited financial reports and grant information returns are released.

LGIRS has established a benchmark score of 70 for the LGFI. Scores below this benchmark indicate that an entity may warrant further consideration in relation to its financial position. Looking back, the LGFI for the Shire of Coolgardie had been declining for some time, indicating emerging concerns well before the issues became public in June 2025, acknowledging that the department had been engaging with the Shire, and our Office, since early 2024 in respect of a variety of concerns identified by them through other available information.

Financial analysis

For 2025, we analysed the current ratios of all local government entities with audits finalised by 31 December 2025. The current ratio is an indicator of an entity's ability to meet its short-term obligations for payment, with a ratio of less than one suggesting that an entity owes more in the short term than it may be able to afford to pay. Four entities recorded a current ratio of less than one (2024: 2; 2023: 1). The four entities with ratios less than one were:

- Shire of Coolgardie
- Shire of Derby-West Kimberley
- Shire of Irwin
- Shire of Victoria Plains.

A further 13 entities reported a ratio between 1 and 2 (2024: 11; 2023: 13), which also indicates potential financial pressure.

Appendix 9 contains a complete listing of the current ratio for each entity for 2024 and 2025.

Case study 2: Historical financial viability concerns at the Shire of Coolgardie

For 2025, the Shire of Coolgardie recorded a current ratio of 0.57. Given the heightened concern with the Shire's financial viability, we performed further audit procedures to satisfy ourselves that the going concern basis for preparation of the financial report was appropriate and a material uncertainty was not required to be included in the audit report. The procedures included:

- deeper and more intensive analysis of cashflow forecasts
- review of budgets
- status of financial facilities
- asset disposal alternatives
- year to date actual financial information for 2026.

[12] Government of Western Australia, *MyCouncil*, mycouncil.wa.gov.au, n.d., 9 February 2026.

Entities hovering around a score of one or trending downwards, should pay particular attention to their cashflow needs and forecasts. Sector-wide results also show a gradual decline. The sector-average current ratio decreased from 5.5 in both 2023 and 2024 to 5.0 in 2025. Median ratios similarly declined from 4.1 in 2023 to 3.75 in 2024 and 3.63 in 2025. The decline in the median indicates that this trend is not driven by outliers but reflects a broader sector decline in entities' ability to meet their short-term payment obligations.

While a number of entities report large surpluses each year, the sector is facing increasing cost pressures with a limited ability for entities to expand their revenue base. Local governments will need to closely monitor their financial outlays and positions to ensure they can continue to deliver essential community services and maintain appropriate levels of investment in their community infrastructure.

Valuations

This year we encountered several instances where a valuer did not comply with the LGIRS (previously the Department of Local Government, Sports and Cultural Industries) directive requiring the use of the market approach for valuing land, including the consideration of public sector restrictions. In all cases, entities were unaware that their valuations were non-compliant with the above requirements, resulting in additional auditor involvement to resolve the matter with the valuer. Adjustments were required to valuations and financial reports.

Assets (PPE and infrastructure) are generally the largest balances in the financial report, meaning that errors in this area tend to be large and carry significant exposure for entities. This is also an area where we see significant numbers of prior period errors, as discussed in the quality section of this report[13].

For several years, we have recommended LGIRS develop and finalise their valuation guidance for the sector. We have provided input on various drafts since September 2023; and this guide has recently been published on 5 March 2026. This guidance will support a consistent understanding of valuation obligations and improve valuation practices generally. Ahead of their 2026 audits, entities should review this guidance to ensure their compliance with the guidelines.

Advocacy and reform

We engage closely with stakeholders and maintain a sector-wide view of emerging risks and systemic issues through our ongoing liaison with key stakeholders. This enabled us to raise with LGIRS a duplication in review requirements. As a result, regulation 5(2)(c)[14] of the Local Government (Financial Management) Regulations 1996, which required a three-yearly CEO review of the appropriateness and effectiveness of financial management systems, was removed effective 1 January 2026. Enhancements have been made to the remaining review obligations under regulations 16 and 17 of the Local Government (Audit) Regulations 1996.

Further reforms have also progressed, importantly the Local Government Inspector has been established to strengthen the regulation of council members and local government staff conduct. In addition, audit committees have been re-constituted as audit, risk and improvement committees, with a requirement for an independent chair to enhance objectivity, accountability and oversight across the sector.

[13] Prior period errors are increasing.

[14] Government of Western Australia, *Local Government Regulations Amendment Regulations (No 4) 2025*, Western Australian Legislation, 17 Dec 2025, 9 February 2026.

We welcome these regulatory changes, which streamline oversight and reduce unnecessary administrative burden on entities. We hope to see positive impacts from these changes when we audit entities.

Governance expectations

We are often asked to meet separately with the council outside of entrance and exit meetings and may also be asked to attend the annual electors meeting. The requests stem from the requirement in 7.12A of the *Local Government Act 1995*, which requires a local government to meet with the auditor of the local government at least once in every year. LGIRS advice is if council formally delegated this responsibility, a meeting between the audit, risk and improvement committee and the auditor would satisfy this requirement.

Meeting with the auditors should occur in a non-public audit entrance and/or exit meeting. This is so conversations can occur outside of normal standing order meeting protocols and confidential matters can be discussed. These are the forum for members of council, the audit committee and administration to speak to their auditors. They are meetings to discuss risks, issues, progress, status and results. It's important these meetings are closed to the public to maintain confidentiality around audit sensitivities and to ensure public or media enquiries are addressed to the Auditor General directly for consideration, rather than audit staff.

We plan to provide guidance on meeting attendance to support a consistent approach to audit related meetings across the sector. This will help streamline processes for entities and ensure best value for money.

We are often asked by entities to meet pre-determined deliverable dates to attend meetings with council, audit, risk and improvement committees, and electors. This can become challenging when there are delays in the audit process. These delays are commonly linked to issues with entity work papers supporting the financial report, or matters requiring formal technical resolution. Greater flexibility from councils is appreciated when necessary to ensure timelines remain reasonable and achievable. The alternative is to stay with the set meetings and report based on the status at that point and specify what is outstanding and plan to resolution.

OAG insights and tips

Our observations from the year are largely unchanged from previous years, indicating entities need continued refinement of their operations.

Streamline the audit process

Entities should:

1. Submit good quality, reviewed and CEO-signed financial reports for audit, no later than 30 September. Earlier submission is encouraged. CEO certification should indicate that management and those charged with governance are satisfied the financial report is complete, accurate and supported by underlying work papers. Supporting work papers and reconciliations should be available when financial reports are lodged. All content should be error free.
2. Communicate to the auditor their assessment of the significance of errors and determine whether adjustments are required. Entities should also analyse the root cause of identified errors.
3. Communicate delays to financial report submission early to minimise disruptions and enable effective resource allocation. Flexibility may be required when rescheduling audits.
4. Evaluate opportunities to submit financial reports earlier for audit.
5. Exercise greater flexibility around committee and council meeting times.
6. Ensure council attend audit entrance and exit meetings with the audit, risk and improvement committee, or that an appropriate delegation is in place. Audit entry and exit meetings are not intended to be part of public proceedings, but are undertaken to communicate audit plans, timeframes and findings with relevant entity staff and committee members.

Better support for entities

The Department of Local Government, Industry Regulation and Safety (LGIRS) should:

7. Update LGFI data on the MyCouncil website as a priority following audit finalisation
8. Consider LGFI information along with other intelligence to proactively intervene and support entities with challenges.

LGIRS response to 7 and 8:

LGIRS recognises the importance of timely publication and updates LGFI data on the MyCouncil website once governance and quality assurance processes are completed. For future reporting years, LGFI data will be published by the end of April following finalisation of audited financial statements by 31 December and receipt of grant information by the end of February each year. This timing will be communicated to local governments via an LG Alert and on the MyCouncil website.

LGIRS continues to strengthen its governance and quality assurance processes to support timely reporting and enhanced transparency, including clearer internal verification milestones, more structured follow-up with local governments, and improved monitoring and oversight arrangements, in coordination with the Local Government Inspector where appropriate. These measures support earlier identification of emerging risks and more proactive engagement with local governments. LGFI information is considered within a

broader monitoring and assurance framework and is assessed alongside audit outcomes, compliance activity and direct engagement, rather than in isolation.

The Local Government Inspector has the statutory powers to intervene where this is considered necessary. Any proactive engagement or intervention is undertaken in a measured and proportionate manner, having regard to the specific circumstances of each local government. LGIRS' approach is focused on the early identification of risk and the provision of guidance and support to assist local governments in addressing emerging challenges.

Improve reporting and accounting for fixed assets

Entities should:

9. Conduct asset counts/stocktakes to support the completeness and accuracy of asset records.

10. Review the newly released LGIRS valuation guide to ensure compliance.

Reduce financial report errors, versions and management letter findings

Entities should:

11. Establish robust financial report quality control procedures, incorporating review by the audit, risk and improvement committee and council.

12. Seek appropriate and timely independent advice when unsure on accounting and disclosure obligations.

13. Alert OAG audit engagement leaders to new processes or systems, issues encountered during the year, or any area of concern or technical accounting determinations.

LGIRS should:

14. Provide guidance for entities via model accounts on how to account for prior period errors.

LGIRS response to 14:

Guidance on the correction of prior period errors is included in the Guidance Material Annual Financial Report Models (2025) for Class 1 and 2 local governments and for Class 3 and 4 local governments. This guidance references the relevant disclosure and retrospective application requirements under AASB 101 and AASB 108.

While the existing material provides an appropriate framework, it is acknowledged that additional practical guidance may assist entities in applying these requirements in particular circumstances. Further enhancements to the guidance are being considered for inclusion in the 2026 annual guidelines. Where a local government identifies a material prior period error, early engagement with LGIRS is expected. While this expectation is not currently formalised in published guidance, it will be communicated through an LG Alert accompanying the updated annual Model Financial Statements, which will be published in Q2 of 2026.

LGIRS will provide guidance as required, including examples where appropriate, to support compliance with the applicable accounting and disclosure requirements. This approach maintains consistency with the existing legislative and accounting framework while allowing LGIRS to provide targeted and proportionate support based on the specific circumstances of each case.

Resources

OAG provide various tools to assist entities with audit readiness and better practice and are available on our website:

- Audit Readiness Tool
- Prepared by client listing
- Financial statements review
- Going concern assessment
- Western Australian Public Sector Audit Committees –Better Practice Guide
- Better practice guidance

LGIRS provide the following to assist entities monitor their performance and prepare their financial report.

- Government of Western Australia, *MyCouncil*, mycouncil.wa.gov.au, n.d., 9 February 2026.
- Department of Local Government, Industry Regulation and Safety, *Financial policy and accounting*, dlsgsc.wa.gov.au, 5 March 2026, 9 February 2026.

Appendix 1: Status and timeliness of audits

Type of audit opinion	
Clear (unmodified)	
Clear opinion with emphasis of matter, matter of significance paragraph or material uncertainty related to going concern	
Material uncertainty related to going concern	
Qualified or a disclaimer of opinion	
Qualified opinion with an emphasis of matter, matter of significance paragraph or material uncertainty related to going concern	

Financial report timeliness – audit ready submissions*	
Received financial report by statutory deadline of 30 September 2025 and assessed audit ready	
Received an extension from DLGSC to the statutory deadline and met this extension with audit ready financial report	
Extension or statutory deadline was not met with audit ready financial report	

** Financial report initially provided may not be of a quality that is audit ready. The icon in the table below reflects the date we assessed the financial report as audit ready.*

Entities listed in alphabetical order with opinion type, opinion date and audit ready financial report submission status.

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
1	Catalina Regional Council	Other		24/09/2025	
2	City of Albany	1		4/12/2025	
3	City of Armadale	1		12/12/2025	
4	City of Bayswater	1		1/12/2025	
5	City of Belmont	1		21/11/2025	
6	City of Bunbury	1		19/11/2025	
7	City of Busselton	1		19/11/2025	
8	City of Canning	1		3/12/2025	
9	City of Cockburn	1		26/11/2025	
10	City of Fremantle	1		3/12/2025	
11	City of Gosnells	1		5/12/2025	
12	City of Greater Geraldton	1		4/12/2025	

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
13	City of Joondalup	1	✓	17/11/2025	✓
14	City of Kalamunda	2	✓	12/11/2025	✗
15	City of Kalgoorlie-Boulder	1	✓	8/12/2025	✗
16	City of Karratha	1	✓	28/11/2025	✓
17	City of Kwinana	1	✓	25/11/2025	✓
18	City of Mandurah	1	✓	11/12/2025	✓
19	City of Melville	1	✓	15/12/2025	✗
20	City of Perth	1	✓	28/11/2025	✓
21	City of Rockingham	1	✓	24/10/2025	✓
22	City of South Perth	2	✓	12/11/2025	✓
23	City of Stirling	1	✓	16/12/2025	✓
24	City of Subiaco	2	✓	5/12/2025	✗
25	City of Swan	1	✓	25/11/2025	✓
26	City of Vincent	2	✓	14/11/2025	✓
27	City of Wanneroo	1	✓	19/11/2025	✓
28	Eastern Metropolitan Regional Council	Other	✓	7/10/2025	✓
29	Mindarie Regional Council	Other	✓	10/11/2025	✓
30	Murchison Regional Vermin Council	Other	✓	12/12/2025	✓
31	Resource Recovery Group	Other	✓	18/12/2025	✗
32	Rivers Regional Council	Other	✓	21/02/2025	✓
33	Shire of Ashburton	2	✓	21/11/2025	✗
34	Shire of Augusta-Margaret River	2	✓	14/11/2025	✓
35	Shire of Beverley	4	✓	4/11/2025	✓
36	Shire of Boddington	4	✓	8/12/2025	✓
37	Shire of Boyup Brook	4	✗	19/12/2025	✓
38	Shire of Bridgetown-Greenbushes	3	✓	8/12/2025	✓
39	Shire of Brookton	4	✓	20/11/2025	✓

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
40	Shire of Broome	2	✓	2/12/2025	✗
41	Shire of Broomehill-Tambellup	4	✓	5/11/2025	✓
42	Shire of Bruce Rock	4	✓	8/12/2025	✓
43	Shire of Capel	3	✓	3/12/2025	✓
44	Shire of Carnamah	4	✓	5/12/2025	✗
45	Shire of Carnarvon	2	✓	5/12/2025	✓
46	Shire of Chapman Valley	4	✓	4/12/2025	✓
47	Shire of Chittering	3	✓	8/12/2025	✓
48	Shire of Christmas Island	3	✓	4/12/2025	✓
49	Shire of Collie	3	✓	19/12/2025	✗
50	Shire of Coolgardie	3	✓	3/12/2025	✓
51	Shire of Corrigin	4	✓	24/11/2025	✓
52	Shire of Cranbrook	4	✓	11/11/2025	✓
53	Shire of Cuballing	4	✓	4/12/2025	✓
54	Shire of Cue	4	✓	8/12/2025	✓
55	Shire of Cunderdin	4	✓	8/12/2025	✓
56	Shire of Dandaragan	3	✓	4/12/2025	✓
57	Shire of Dardanup	3	✓	21/11/2025	✓
58	Shire of Denmark	3	✓	3/12/2025	✓
59	Shire of Derby-West Kimberley	2	✓	24/11/2025	✓
60	Shire of Donnybrook Balingup	3	✓	9/12/2025	✓
61	Shire of Dowerin	4	✓	10/12/2025	✓
62	Shire of Dumbleyung	4	✓	4/12/2025	✓
63	Shire of Dundas	4	✓	10/12/2025	✗
64	Shire of East Pilbara	2	✓	27/11/2025	✗
65	Shire of Esperance	2	✓	5/12/2025	✓
66	Shire of Exmouth	3	✓	3/12/2025	✓

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
67	Shire of Gingin	3	✓	20/11/2025	✓
68	Shire of Gnowangerup	4	✓	21/11/2025	✓
69	Shire of Goomalling	4	✓	26/11/2025	✓
70	Shire of Harvey	2	✓	20/11/2025	✓
71	Shire of Irwin	3	✓	1/12/2025	✓
72	Shire of Jerramungup	4	✓	27/11/2025	✓
73	Shire of Katanning	3	✓	10/12/2025	✓
74	Shire of Kellerberrin	4	✓	25/11/2025	✓
75	Shire of Kent	4	✓	2/12/2025	✓
76	Shire of Kojonup	3	✓	2/12/2025	✓
77	Shire of Kondinin	4	✓	5/12/2025	✓
78	Shire of Koorda	4	✓	16/10/2025	✓
79	Shire of Kulin	4	✓	5/12/2025	✓
80	Shire of Lake Grace	4	✓	25/11/2025	✓
81	Shire of Laverton	3	✓	5/12/2025	✓
82	Shire of Leonora	3	✓	22/12/2025	✗
83	Shire of Manjimup	2	✓	25/11/2025	✓
84	Shire of Meekatharra	3	✓	18/12/2025	✓
85	Shire of Menzies	4	✓	21/11/2025	✓
86	Shire of Merredin	3	✓	25/11/2025	✗
87	Shire of Mingenew	4	✓	24/11/2025	✓
88	Shire of Moora	3	✓	28/11/2025	✓
89	Shire of Morawa	4	✓	27/11/2025	✗
90	Shire of Mount Marshall	4	✓	1/12/2025	✓
91	Shire of Mukinbudin	4	✓	13/11/2025	✓
92	Shire of Mundaring	2	✓	2/12/2025	✓
93	Shire of Murchison	4	✓	27/11/2025	✓

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
94	Shire of Murray	2	✓	18/11/2025	✓
95	Shire of Nannup	4	✓	4/12/2025	✓
96	Shire of Narembeen	4	✓	28/11/2025	✓
97	Shire of Narrogin	3	✓	14/11/2025	✓
98	Shire of Ngaanyatjarraku	4	✓	4/12/2025	✓
99	Shire of Northam	2	✓	1/12/2025	✓
100	Shire of Northampton	3	✓	15/12/2025	✓
101	Shire of Nungarin	4	✓	3/12/2025	✓
102	Shire of Peppermint Grove	4	✓	27/11/2025	✓
103	Shire of Perenjori	4	✓	4/12/2025	✓
104	Shire of Pingelly	4	✓	19/12/2025	✗
105	Shire of Plantagenet	3	✓	15/12/2025	✓
106	Shire of Quairading	4	✓	4/12/2025	✓
107	Shire of Ravensthorpe	3	✓	4/12/2025	✓
108	Shire of Sandstone	4	✓	15/12/2025	✓
109	Shire of Serpentine-Jarrahdale	2	✓	12/11/2025	✓
110	Shire of Shark Bay	4	✓	11/12/2025	✓
111	Shire of Tammin	4	✓	2/12/2025	✗
112	Shire of Three Springs	4	✓	2/12/2025	✓
113	Shire of Toodyay	3	✗	23/12/2025	✗
114	Shire of Trayning	4	✓	2/12/2025	✓
115	Shire of Upper Gascoyne	4	✓	5/12/2025	✓
116	Shire of Victoria Plains	4	✓	28/11/2025	✓
117	Shire of Wagin	4	✓	14/11/2025	✓
118	Shire of Wandering	4	✓	15/12/2025	✓
119	Shire of Waroona	3	✓	21/11/2025	✓
120	Shire of West Arthur	4	✓	10/12/2025	✓

	Entity	Band	Type of opinion	Opinion issued	Audit ready submission of financial report
121	Shire of Westonia	4	✓	4/12/2025	✓
122	Shire of Wickepin	4	✓	4/12/2025	✓
123	Shire of Williams	4	✓	9/12/2025	✓
124	Shire of Wiluna	4	✓	2/12/2025	✓
125	Shire of Wongan-Ballidu	4	✓	12/12/2025	✗
126	Shire of Woodanilling	4	✓	4/12/2025	✓
127	Shire of Wyalkatchem	4	✓	28/11/2025	✓
128	Shire of Wyndham-East Kimberley	2	✓	25/11/2025	✓
129	Shire of Yilgarn	3	✓	9/10/2025	✓
130	Shire of York	3	✓	27/11/2025	✓
131	Town of Bassendean	3	✓	14/11/2025	✓
132	Town of Cambridge	2	✓	4/12/2025	✓
133	Town of Claremont	3	✓	10/12/2025	✗
134	Town of Cottesloe	3	✓	3/12/2025	✗
135	Town of Mosman Park	3	✓	8/12/2025	✓
136	Town of Port Hedland	1	✓	17/12/2025	✗
137	Town of Victoria Park	2	✓	8/12/2025	✓
138	Western Metropolitan Regional Council	Other	✓	17/10/2025	✓

Source: OAG

Opinion type by entity band allocations

Band of entity	Number of entities	Opinions issued	Clean opinions	Modified opinions	Opinions including EoM paragraphs
Band 1	23 (23)	23 (23)	23 (22)	0 (1)	6 (4)
Band 2	21 (21)	20 (21)	20 (20)	0 (1)	6 (5)
Band 3	35 (35)	32 (35)	31 (32)	1 (3)	5 (5)
Band 4	60 (60)	56 (59)	55 (52)	1 (7)	3 (5)
Other (e.g. councils)	8 (8)	7 (8)	7 (7)	0 (1)	2 (1)
Total	**147 (147)**	**138 (146)**	**136 (133)**	**2 (13)**	**22 (20)**

Source: OAG

Notes: 2024 numbers included in brackets.

Audits from prior years finalised in 2025

Entity	Balance date	Opinion issued	Opinion type
City of Greater Geraldton	30 June 2024	28 March 2025	✓
City of Nedlands*	30 June 2024	5 September 2025	✗✓
Shire of Bridgetown Greenbushes	30 June 2024	4 April 2025	✓
Shire of Collie	30 June 2024	20 May 2025	✓
Shire of Coolgardie	30 June 2024	23 June 2025	✓✓
Shire of Dundas	30 June 2024	9 April 2025	✓
Shire of Halls Creek*	30 June 2024	19 December 2025	✗
Shire of Nannup	30 June 2024	4 February 2025	✗
Shire of Toodyay	30 June 2024	13 June 2025	✗
Shire of Wickepin	30 June 2024	14 February 2025	✗
Town of Cottesloe	30 June 2024	14 February 2025	✓✓

Source: OAG

** These entities audits are also delayed for 2025 and were included in our Status of Local Government Audits 2025 report*[15]

[15] Office of the Auditor General, *Status of Local Government Audits 2025*, OAG website, 28 January 2026.

Appendix 2: Entities who received an extension from LGIRS to submit their financial report after the 30 September legislated deadline

Entity	Approved extension date
Resource Recovery Group	17 October 2025
Shire of Dundas	3 November 2025
Shire of Halls Creek	18 December 2025
Shire of Leonora	31 October 2025
Shire of Merredin	14 October 2025
Shire of Toodyay	1 October 2025
Shire of Wongan-Ballidu	10 October 2025
Town of Cottesloe	13 October 2025
Town of East Fremantle	31 October 2025

Source: LGIRS

Appendix 3: Qualified and disclaimer of opinions

2025 qualifications

Entity	Details of qualification
Shire of Boyup Brook	**Biological assets** We were unable to obtain sufficient appropriate audit evidence to verify the existence and number of biological assets at 30 June 2024, nor were we able to confirm the biological assets by alternative means. Our audit opinion on the annual financial report for the period ending 30 June 2024 was modified accordingly. Since the closing balance at 30 June 2024 of biological assets is the opening balance at 1 July 2024 and forms the basis for the determination of operations for the year, we were unable to determine whether any adjustments to the operations net result for the year ended 30 June 2025 may be necessary.
Shire of Toodyay	**Financial report comparative information not supported with complete and accurate underlying records** We were unable to obtain sufficient and appropriate audit evidence regarding the prior year financial report, as the financial report was submitted for audit purposes without complete and accurate underlying records. Our opinion on the financial report for the year ended 30 June 2024 was modified accordingly. Our opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current year's figures and the corresponding figures.
	Cash and cash equivalents The Shire's bank reconciliation at 30 June 2025 included an unreconciled balance of $22,991. We were unable to confirm this figure by alternative means and consequently were unable to determine whether any adjustments were necessary on cash and cash equivalents at 30 June 2025.
	Restatement of corresponding figures We were unable to obtain sufficient and appropriate audit evidence for the restatement of corresponding figures as set out in Note 28. We were unable to confirm these restatements by alternative means and consequently were unable to determine whether any adjustments were necessary to Note 28. In addition, Note 28 does not comply with the disclosure requirements of AASB 108 Accounting Policies, Changes in Accounting Estimates and Errors, and it did not include all corrected line items in the statement of cash flow and the statement of financial activity.

Source: OAG

Delayed 2024 qualified and disclaimer of opinions

The below list of qualified and disclaimer of opinions is for those entities listed in Appendix 1 which had their 2024 audits finalised in 2025.

Entity	Details of qualification or disclaimer
City of Nedlands	**Qualification** **Financial report comparative information not supported with complete and accurate underlying records** We were unable to obtain sufficient and appropriate audit evidence regarding the prior year financial report, as the financial report was submitted for audit purposes without complete and accurate underlying records. The opinion on the financial report for the year ended 30 June 2023 was modified accordingly. The opinion on the current year financial report is also modified because of the

Entity	Details of qualification or disclaimer
	possible effect of this matter on the comparability of the current year's figures and the corresponding figures.
Shire of Halls Creek	**Qualification** **Financial report comparative information not supported with complete and accurate underlying records** We were unable to obtain sufficient and appropriate audit evidence regarding the prior year financial report, as the financial report was submitted for audit purposes without complete and accurate underlying records. The opinion on the financial report for the year ended 30 June 2023 was modified accordingly. The opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current year's figures and the corresponding figures.
	Qualification **Restatement of corresponding figures** We were unable to obtain sufficient and appropriate audit evidence for the restatement of corresponding figures as stated in the Statement of Comprehensive Income, Statement of Cash Flows, Statement of Financial Activity and Note 28 of the financial report. We were unable to confirm these restatements by alternative means and consequently were unable to determine whether any adjustments were necessary on the corresponding figures of these statements.
	Qualification **Infrastructure assets not revalued as required by the Local Government (Financial Management) Regulations** Other Infrastructure assets reported at the carrying values of $6,460,241 and $6,963,171 as at 30 June 2023 and 30 June 2022 respectively in Note 9 (a) of the financial report have not been revalued as required by Regulation 17A(4A)(b) of the Local Government (Financial Management) Regulations 1996 since 30 June 2018. Consequently, we were unable to determine the extent to which the carrying amounts of other infrastructure assets are misstated, as it was impracticable to do so. Additionally, we are unable to determine whether there may be any consequential impact on Revaluation Surplus as at 30 June 2023 and 30 June 2022, as well as Depreciation, Net Result for the Period and Retained Surplus as at 30 June 2023.
Shire of Nannup	**Qualification** **Land and buildings and infrastructure** The opinion in the prior year was qualified because land, buildings and infrastructure with carrying values of $1,615,000, $8,737,435 and $100,957,611 respectively disclosed in Notes 8(a) and 9(a) of the financial report as at 30 June 2023, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures.
Shire of Wickepin	**Qualification** **Infrastructure asset valuation** The opinion in the prior year was qualified because infrastructure assets reported at the carrying value of $92,213,435 as disclosed in Note 7(a) as at 30 June 2023, had not been revalued as required by the Regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is modified because of the possible effects of this matter on the comparability of the current period's figures and the corresponding figures.

Entity	Details of qualification or disclaimer
Shire of Toodyay	**Disclaimer** **Financial report not supported with complete and accurate underlying records** We were unable to obtain sufficient appropriate audit evidence regarding the financial report as a whole, as the financial report was submitted for audit purposes without complete and accurate underlying records. We were unable to audit the financial report by alternative means. Consequently, we are unable to determine whether any adjustments were necessary to the financial report as a whole for the year ended 30 June 2024.

Source: OAG

Appendix 4: Prior year qualifications and disclaimers removed in 2025

Entity	Details of prior year qualification
Shire of Goomalling	**Infrastructure** The opinion in the prior year was qualified because infrastructure asset classes of roads, drainage and footpaths (as disclosed in note 8(a) of the financial report at 30 June 2023) with the carrying values of $40,811,938, $2,153,484 and $770,060 respectively, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effects of this matter on the comparability of the current period's figures and the corresponding figures.
Shire of Kent	**Infrastructure** The opinion in the prior year was qualified because other infrastructure assets (as disclosed in note 9(a) of the financial report at 30 June 2023) with a carrying value of $4,867,091, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures.
Shire of Nannup	**Land and buildings and infrastructure** The opinion in the prior year was qualified because land, buildings and infrastructure assets (disclosed in notes 8(a) and 9(a) of the financial report at 30 June 2023) with carrying values of $1,615,000, $8,737,435 and $100,957,611 respectively, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures.
Shire of Westonia	**Infrastructure** The opinion in the prior year was qualified because infrastructure assets (as disclosed in note 9(a) of the financial report at 30 June 2023) with a carrying value of $43,562,879, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures.
Shire of Wickepin	**Infrastructure assets valuation** The opinion in the prior year was qualified because infrastructure assets (as disclosed in note 7(a) of the financial report at 30 June 2023) reported at the carrying value of $92,213,435, had not been revalued as required by the regulations. The Shire was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is modified because of the possible effects of this matter on the comparability of the current period's figures and the corresponding figures.
Town of Port Hedland	**Infrastructure assets valuations** The Town did not recognise 670 (2023:797) infrastructure assets with a value of $17,371,521 (2023: $25,112,117) in accordance with the Regulation 17A(2)(a) of the Local Government Financial Management Regulations 1996, as these assets could not be located due to weaknesses in the asset management system. The assets were instead adjusted to a nil carrying value while still being in use and accounted for in the asset register. We were unable to determine the

Entity	Details of prior year qualification
	impact on the net carrying amount of infrastructure assets and the consequential impact on retained earnings, revaluation reserves, depreciation and net surplus for the year, as it is impracticable to do so. In addition, the opinion in the prior year was qualified because drainage and other infrastructure assets, reported at a carrying value of $33,243,203 and $47,582,860 respectively (as disclosed in note 9 to the financial statements at 30 June 2023), were not all revalued as required by the regulations. The Town was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures. **Investment property** The opinion in the prior year was qualified because investment property (as disclosed in note 12 of the financial report at 30 June 2023) with the carrying value of $45,027,262, had not been revalued as required by the regulations. The Town was unable to correct these prior year figures in the current year. Consequently, the opinion on the current year financial report is also modified because of the possible effect of this matter on the comparability of the current period's figures and the corresponding figures.

Source: OAG

Entity	Details of prior year disclaimer
Shire of Toodyay	**Financial report not supported with complete and accurate underlying records** We were unable to obtain sufficient appropriate audit evidence regarding the financial report as a whole, as the financial report was submitted for audit purposes without complete and accurate underlying records. We were unable to audit the financial report by alternative means. Consequently, we were unable to determine whether any adjustments were necessary to the financial report as a whole for the year ended 30 June 2024.

Source: OAG

Appendix 5: Emphasis of matter paragraphs included in auditor reports

2025 emphasis of matter paragraphs

Entity	Description of EoM paragraphs
City of Bayswater	**Investment in Associates** We draw attention to note 27 to the financial report, which states that effective 1 July 2025, two member participants have resolved to withdraw as member participants from Eastern Metropolitan Regional Council effective from 1 July 2025. The City continues to be a member council participant. Our opinion is not modified in respect of this matter.
City of Busselton	**Restatement of Comparative balances** We draw attention to Note 32 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
City of Joondalup	**Restatement of Comparative balances** We draw attention to Note 26 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in these financial statements. Our opinion is not modified in respect of this matter.
City of Kwinana	**Restatement of comparative figures** We draw attention to Note 32 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
City of Subiaco	**Restatement of comparative balances** We draw attention to Note 31 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
City of Swan	**Investment in Associates** We draw attention to Note 25 to the financial report, which states that the City has resolved to withdraw as a member participant from Eastern Metropolitan Regional Council effective from 1 July 2025. Our opinion is not modified in respect of this matter.
Rivers Regional Council	**Basis of accounting** We draw attention to Note 1 of the financial report, which discloses that the Council has decided to wind up Rivers Regional Council. Consequently, the financial report has been prepared on a liquidation basis. Our opinion is not modified in respect of this matter.
Shire of Bruce Rock	**Restatement of comparative balances** We draw attention to Note 30 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Coolgardie	**Restatement of comparative figures** We draw attention to Note 31 to the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated

Entity	Description of EoM paragraphs
	and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Dardanup	**Restatement of comparative balances** We draw attention to Note 30 of the financial statements which states that the amounts reported in the previously issued 30 June 2024 financial statements have been restated and disclosed as comparatives in these financial statements. Our opinion is not modified in respect of this matter.
Shire of Denmark	**Restatement of Comparative balances** We draw attention to Note 29 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Manjimup	**Restatement of Comparative Balances** We draw attention to Note 30 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Meekatharra	**Restatement of Comparative balances** We draw attention to Note 25 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Mundaring	**Investment in Associates** We draw attention to Note 22 to the financial report, which states that the Shire has resolved to withdraw as a member participant from Eastern Metropolitan Regional Council effective from 1 July 2025. Our opinion is not modified in respect of this matter.
Shire of Serpentine-Jarrahdale	**Correction of Error** We draw attention to Note 34 of the financial report which states that previously unrecognised assets have been recognised prospectively at 30 June 2025 as retrospective restatement was impracticable. Our opinion is not modified in respect of this matter.
Shire of Shark Bay	**Restatement of Comparative Balances** We draw attention to Note 27 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Shire of Williams	**Restatement of comparative figures** We draw attention to Note 29 to the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Resource Recovery Group	**Basis of Accounting** We draw attention to Note 1 of the financial report which describes the basis of accounting and that the financial report has been prepared on a non-going concern basis for the reasons set out therein. Our opinion is not modified in respect of this matter.
Town of Bassendean	**Investment in Associates** We draw attention to Note 22 to the financial report, which states that effective 1 July 2025, two member participants have resolved to withdraw as member

Entity	Description of EoM paragraphs
	participants from Eastern Metropolitan Regional Council effective from 1 July 2025. The Town continues to be a member council participant. Our opinion is not modified in respect of this matter.
Town of Cambridge	**Restatement of Comparative Balances** We draw attention to Note 31 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Town of Port Hedland	**Restatement of comparative figures** We draw attention to Note 33 to the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.
Town of Victoria Park	**Restatement of comparative figures** We draw attention to Note 30 of the financial report which states that the amounts reported in the previously issued 30 June 2024 financial report have been restated and disclosed as comparatives in these financial statements. Our opinion is not modified in respect of this matter.

Source: OAG

2024 delayed emphasis of matter paragraphs

The below list of emphasis of matter paragraphs is for those entities listed in Appendix 1 which had their 2024 audits finalised in 2025.

Entity	Description of EoM paragraphs
City of Nedlands	**Restatement of assets, liabilities and equity as at 1 July 2023** We draw attention to Note 29 of the financial report which states that historical errors in assets, liabilities and equity amounts reported have been corrected in opening balances as at 1 July 2023 in this financial report. Our opinion is not modified in respect of this matter.
Town of Cottesloe	**Restatement of Comparative balances** We draw attention to Note 30 of the financial report which states that the amounts reported in the previously issued 30 June 2023 financial report have been restated and disclosed as comparatives in this financial report. Our opinion is not modified in respect of this matter.

Source: OAG

Appendix 6: Delayed 2024 audit material uncertainty related to going concern paragraph

The below list of material uncertainty relating to going concern (MURGC) paragraph is for those entities listed in Appendix 1 which had their 2024 audits finalised in 2025.

Entity	Description of MURGC paragraph
Shire of Coolgardie	**Material uncertainty related to going concern** We draw attention to Note 1 in the financial report, which indicates that the Shire incurred a net loss of $4,617,984 for the year ended 30 June 2024 and as of that date, the Shire's current liabilities exceeded its current assets by $14,210,643 and the unrestricted cash balance was overdrawn by $934,081. As stated in Note 1, these events, or conditions, along with other matters as set forth in Note 1, indicate that a material uncertainty exists that may cast significant doubt on the Shire 's ability to continue as a going concern. The audit opinion is not modified in respect of this matter.

Source: OAG

Appendix 7: Local government certifications issued since September 2025

Certifications issued for 2025

Entity and opinion	Opinion issued
City of Bayswater	
Local Roads and Community Infrastructure Program (Phases 1-4)	31 October 2025
City of Mandurah	
Roads to Recovery	5 November 2025
Local Roads and Community Infrastructure Program (Phase 4)	5 November 2025
City of Busselton	
Roads to Recovery	14 November 2025
Local Roads and Community Infrastructure Program	14 November 2025

Source: OAG

Outstanding certifications issued from 2021-22

Entity and opinion	Opinion issued
Shire of Halls Creek	
Local Roads and Community Infrastructure Program	23 December 2025

Source: OAG

Note: the cut-off date is 24 March 2026.

Appendix 8: Other local government opinions issued since September 2025

Entity	Opinion issued
Shire of Yalgoo 2023	19 February 2026
Shire of Yalgoo 2024	19 February 2026
Shire of Dalwallinu	23 March 2026

Source: OAG

Note: the cut-off date for this appendix is 24 March 2026.

Appendix 9: Local government current ratios for 2025

Below are the calculated current ratios for each local government for the past two years. The current ratio calculated as the current assets divided by current liabilities. A current ratio of less than one means an entity has more current liabilities than current assets, meaning they may not be able to pay their debts as and when they fall due.

Entity	Band	Current ratio 2025	Current ratio 2024
Bunbury-Harvey Regional Council	Other	NCWST	1.70
City of Albany	1	3.30	3.46
City of Armadale	1	3.52	3.11
City of Bayswater	1	4.41	4.27
City of Belmont	1	5.34	6.92
City of Bunbury	1	2.29	2.24
City of Busselton	1	3.90	4.26
City of Canning	1	4.14	4.11
City of Cockburn	1	4.75	5.56
City of Fremantle	1	2.39	2.75
City of Gosnells	1	2.41	3.17
City of Greater Geraldton	1	1.91	2.66
City of Joondalup	1	3.47	3.60
City of Kalamunda	2	3.57	2.78
City of Kalgoorlie - Boulder	1	1.61	2.55
City of Karratha	1	9.15	8.45
City of Kwinana	1	1.90	1.99
City of Mandurah	1	2.35	2.41
City of Melville	1	4.32	5.25
City of Nedlands	2	NCWST	2.31
City of Perth	1	6.10	5.94
City of Rockingham	1	3.40	3.99
City of South Perth	2	3.88	3.55
City of Stirling	1	3.16	2.77
City of Subiaco	2	12.03	9.87
City of Swan	1	4.36	3.57
City of Vincent	2	3.06	2.72
City of Wanneroo	1	4.40	4.90
Eastern Metropolitan Regional Council	Other	1.75	2.32
Mindarie Regional Council	Other	3.28	4.83
Murchison Regional Vermin Council	Other	3.10	2.33

Entity	Band	Current ratio 2025	Current ratio 2024
Rivers Regional Council	Other	8.31	5.06
Shire of Ashburton	2	4.92	4.46
Shire of Augusta-Margaret River	2	2.48	2.77
Shire of Beverley	4	2.70	2.14
Shire of Boddington	4	1.92	1.84
Shire of Boyup Brook	4	2.32	2.91
Shire of Bridgetown-Greenbushes	3	1.70	2.55
Shire of Brookton	4	11.38	10.52
Shire of Broome	2	3.64	4.01
Shire of Broomehill-Tambellup	4	2.89	4.18
Shire of Bruce Rock	4	3.01	3.15
Shire of Capel	3	2.30	4.21
Shire of Carnamah	4	4.07	5.03
Shire of Carnarvon	2	2.17	2.46
Shire of Chapman Valley	4	2.00	2.36
Shire of Chittering	3	2.18	1.89
Shire of Christmas Island	3	2.52	2.45
Shire of Cocos (Keeling) Islands	4	NCWST	9.42
Shire of Collie	3	2.22	1.86
Shire of Coolgardie	3	0.57	0.17
Shire of Coorow	4	NCWST	3.75
Shire of Corrigin	4	10.60	7.10
Shire of Cranbrook	4	5.97	7.99
Shire of Cuballing	4	2.15	2.33
Shire of Cue	4	17.13	12.93
Shire of Cunderdin	4	4.25	7.00
Shire of Dalwallinu	3	NCWST	6.08
Shire of Dandaragan	3	4.81	3.83
Shire of Dardanup	3	2.98	3.53
Shire of Denmark	3	2.49	2.24
Shire of Derby-West Kimberley	2	0.96	0.95
Shire of Donnybrook-Balingup	3	2.82	2.24
Shire of Dowerin	4	5.13	4.87
Shire of Dumbleyung	4	9.66	7.15
Shire of Dundas	4	3.68	5.81
Shire of East Pilbara	2	5.43	7.34
Shire of Esperance	2	5.07	5.32

Entity	Band	Current ratio 2025	Current ratio 2024
Shire of Exmouth	3	8.39	6.71
Shire of Gingin	3	2.70	2.60
Shire of Gnowangerup	4	4.19	5.46
Shire of Goomalling	4	1.07	1.30
Shire of Halls Creek	3	NCWST	2.73
Shire of Harvey	2	2.30	2.35
Shire of Irwin	3	0.92	1.09
Shire of Jerramungup	4	4.32	4.14
Shire of Katanning	3	2.27	2.40
Shire of Kellerberrin	4	2.51	3.43
Shire of Kent	4	12.23	10.26
Shire of Kojonup	3	2.46	1.50
Shire of Kondinin	4	3.90	6.45
Shire of Koorda	4	7.27	6.92
Shire of Kulin	4	4.90	4.04
Shire of Lake Grace	4	7.62	13.96
Shire of Laverton	3	6.17	4.54
Shire of Leonora	3	4.42	3.75
Shire of Manjimup	2	3.42	3.50
Shire of Meekatharra	3	28.45	25.36
Shire of Menzies	4	11.32	11.85
Shire of Merredin	3	4.90	3.25
Shire of Mingenew	4	2.87	2.98
Shire of Moora	3	1.94	3.65
Shire of Morawa	4	6.64	6.61
Shire of Mount Magnet	4	NCWST	5.90
Shire of Mount Marshall	4	4.37	2.85
Shire of Mukinbudin	4	4.83	4.19
Shire of Mundaring	2	3.71	3.89
Shire of Murchison	4	2.26	3.05
Shire of Murray	2	2.38	2.89
Shire of Nannup	4	2.53	2.96
Shire of Narembeen	4	6.14	8.24
Shire of Narrogin	3	3.85	3.41
Shire of Ngaanyatjarraku	4	37.74	10.03
Shire of Northam	2	2.38	2.45
Shire of Northampton	3	1.47	2.10

Entity	Band	Current ratio 2025	Current ratio 2024
Shire of Nungarin	4	5.04	5.93
Shire of Peppermint Grove	4	4.83	4.50
Shire of Perenjori	4	4.69	3.99
Shire of Pingelly	4	2.84	2.09
Shire of Plantagenet	3	3.49	5.41
Shire of Quairading	4	5.38	4.50
Shire of Ravensthorpe	3	3.96	3.80
Shire of Sandstone	4	16.22	32.52
Shire of Serpentine-Jarrahdale	2	2.53	2.56
Shire of Shark Bay	4	6.94	2.70
Shire of Tammin	4	11.07	12.76
Shire of Three Springs	4	7.97	5.34
Shire of Toodyay	3	2.19	2.21
Shire of Trayning	4	6.39	4.31
Shire of Upper Gascoyne	4	3.24	3.30
Shire of Victoria Plains	4	0.81	1.52
Shire of Wagin	4	5.19	6.45
Shire of Wandering	4	1.13	1.55
Shire of Waroona	3	2.60	2.28
Shire of West Arthur	4	4.07	4.46
Shire of Westonia	4	9.74	14.69
Shire of Wickepin	4	8.48	10.74
Shire of Williams	4	3.38	4.82
Shire of Wiluna	4	6.79	11.30
Shire of Wongan-Ballidu	4	4.02	5.87
Shire of Woodanilling	4	3.63	2.95
Shire of Wyalkatchem	4	4.53	14.88
Shire of Wyndam-East Kimberley	2	1.82	3.12
Shire of Yalgoo	4	NCWST	NCWST
Shire of Yilgarn	3	10.45	10.53
Shire of York	3	1.77	2.95
Resource Recovery Group	Other	1.58	1.94
Catalina Regional Council	Other	30.98	93.29
Town of Bassendean	3	2.77	2.55
Town of Cambridge	2	5.89	5.31
Town of Claremont	3	4.25	3.94
Town of Cottesloe	3	2.91	3.05

Entity	Band	Current ratio 2025	Current ratio 2024
Town of East Fremantle	3	NCWST	2.08
Town of Mosman Park	3	3.48	3.17
Town of Port Hedland	1	8.95	12.07
Town of Victoria Park	2	3.60	3.78
Western Metropolitan Regional Council	Other	2.41	2.13

Source: OAG

NCWST: audit not completed within statutory timeframes, data was not available at the cut-off date of this report.

Average current ratio by band

Refer to the below table which shows the average ratio across each band of local government.

Band	2025 Average	2025 Median	2024 Average	2024 Median
Band 1	3.98	3.52	4.35	3.60
Band 2	3.76	3.42	3.73	3.12
Band 3	4.08	2.60	3.89	2.95
Band 4	6.11	4.35	6.38	4.84
Other (regional councils)	7.35	2.76	14.20	2.33
Sector overall	5.00	3.63	5.51	3.75

Source: OAG

Appendix 10: Other certifications issued since September 2025

Certifications issued for 2025

Entity and opinion	Opinion issued
Western Australian Land Authority	
Royalties for Regions - Collie Eco-Concrete Feasibility Study & Peel Business Park Activation - Aryzta Bakery	1 December 2025
Commissioner for Main Roads	
National Partnership on Infrastructure Projects in Western Australia	18 December 2025
Black Spot Projects (*National Land Transport Act 2014*)	18 December 2025
Land Transport Infrastructure Projects (*National Land Transport Act 2014*)	18 December 2025
Department of Local Government, Industrial Relations and Safety	
Local Government Financial Assistance Act 1995	20 January 2026
Department of Creative Industries, Tourism and Sport	
Royalties for Regions– Regional Exhibition Touring Boost Project- Final Report	26 February 2026

Source: OAG

Note: the cut-off date for this appendix is 24 March 2026.

Appendix 11: Other opinions issued since September 2025

Entity and opinion	Opinion issued
Albany Cemetery Board	25 November 2025
Bunbury Cemetery Board	26 November 2025
Electricity Networks Corporation trading as Western Power - agreed upon procedures	17 December 2025
Kalgoorlie-Boulder Cemetery Board	5 December 2025
Keep Australia Beautiful Council (W.A.)	11 November 2025
Trustees of the Public Education Endowment	26 November 2025
Western Australian Greyhound Racing Association	1 December 2025

Source: OAG

Note: the cut-off date for this appendix is 24 March 2026.

Appendix 12: Opinion and management letter definitions

In the auditor's report we include the audit opinion on the annual financial report and any other matters that, in our judgement, need to be highlighted. This year the Auditor General has issued the following types of opinions:

- **Clear opinion**: Indicates satisfactory financial controls. The financial report is based on proper accounts, complies with relevant legislation and accounting standards, and fairly represents performance and financial position.
- **Clear opinion with an EoM:** Draws attention to a matter disclosed in the financial report to aid the readers understanding but does not result in a qualified opinion.
- **Qualified opinion:** Given when the audit identifies materially misleading information, inadequate controls or conflicts with the financial reporting frameworks.
- **Disclaimer of opinion:** The most serious audit outcome, issued when the auditor is unable to form an opinion due to insufficient evidence to form an opinion after all reasonable efforts.

We report weaknesses in the control environment to the CEO, mayor, president or chairperson and the Minister for Local Government. Findings will be rated as significant, moderate or minor. We also indicate if the finding has the potential to impact the audit opinion and if it relates to the prior year and remains unresolved. Both quantitative and qualitative aspects guide our ratings.

Risk category	Audit impact	Management action required
Significant	Findings where there is potentially a significant risk to the entity should it not be addressed by the entity promptly. A significant rating could indicate the need for a modified audit opinion in the current year or in a subsequent reporting period if not addressed. However, even if the issue is not likely to impact the audit opinion, it should be addressed promptly.	Priority or urgent action by management to correct the material misstatement in the financial report to avoid a qualified opinion or for control risks, implement a detailed action plan as soon as possible, within one to two months.
Moderate	Findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.	Control weaknesses of sufficient concern to warrant action being taken as soon as practicable, within three to six months. If not addressed promptly, they may escalate to significant or high risk.
Minor	Those findings that are not of primary concern but still warrant action being taken.	Management to implement an action plan within six to 12 months to improve existing process or internal control.

Source: OAG

We give management the opportunity to review our audit findings and provide comments prior to completion of the audit. Each control finding is documented in a management letter which identifies weakness, implications for the entity, risk category and a recommended improvement action.

Auditor General's 2025-26 reports

Number	Title	Date tabled
13	Local Government 2025 – Financial Audit Results	15 April 2026
12	Local Government 2025 – Information System Audit Results	25 March 2026
11	Local Government Management of Gifts and Benefits	18 March 2026
10	Controls Over Portable Assets – State Entities	6 March 2026
9	Microsoft 365 Security Controls – State Entities	6 March 2026
8	Local Government Audit Status Report	28 January 2026
7	State Government 2025 – Information Systems Audit Results	3 December 2025
6	State Government 2025 – Financial Audit Results	3 December 2025
5	Valuation of Property Held by the Public Education Endowment Trust	3 December 2025
4	WA's Progress to Implement the National Principles for Child Safe Organisations (arising from the Royal Commission into Institutional Responses to Child Sexual Abuse)	27 November 2025
3	Maintaining Regional Local Roads	12 November 2025
2	Gold Corporation – Trade Applications	29 October 2025
1	Management of Housing Maintenance Information	6 August 2025

(Appendix AAR: 10.2F)

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

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Biannual Risk Management Dashboard Report

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Failure to fulfil compliance obligations pursuant to the Local Government (Audit) Regulations 1996, Regulation 17.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 10.4)

RISK ASSESSMENT TOOL

REPORT TITLE: *2026 Governance Health Review*

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)
4 - Document Management Processes
5 - Employment Practices
8 - Errors, Omissions and Delays

RISK ASSESSMENT CONTEXT: Operational

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	Failure to give proper consideration to the reports findings and recommendations could expose the Shire to additional remediation costs.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A
LEGAL AND COMPLIANCE	If audit findings are not appropriately addressed, there is a risk that governance frameworks may not fully align with legislative requirements or better practice, potentially leading to non-compliance and future audit findings.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A
REPUTATIONAL	If governance improvements are not addressed, there is a risk of reduced confidence from stakeholders, which may impact the Shire's reputation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 10.5)

RISK ASSESSMENT TOOL

REPORT TITLE: Financial Management Systems Review- Update Report

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Failure to fulfil obligations pursuant to the Local Government (Financial Management) Regulations 1996, Regulation 5.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 10.6)

RISK ASSESSMENT TOOL

REPORT TITLE: *Network and Internet Outage – 27th March 2026*

RISK THEME PROFILE:

2 - Business and Community Disruption

11 - IT, Communication Systems and Infrastructure

RISK ASSESSMENT CONTEXT: Operational

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	There is exposure to: - Productivity losses during outages - Inefficiencies in service delivery - Potential future costs associated with system upgrades, redundancy measures, or contract improvements	Moderate (3)	Possible (3)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	The outage resulted in a complete loss of internet connectivity across all Shire sites for approximately six hours, impacting access to core systems, communications, and service delivery. There is a risk that similar future outages may: – Disrupt critical services to the community – Limit Council's ability to operate effectively – Impact time-sensitive activities and statutory functions	Moderate (3)	Possible (3)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
LEGAL AND COMPLIANCE	Service disruptions may limit the Shire's ability to: – Meet statutory obligations and reporting timeframes – Maintain required service standards – Fulfil contractual or regulatory requirements While no breach has been identified from this incident, ongoing weaknesses could increase compliance exposure.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Extended outages affecting public-facing services and communications may: – Reduce community confidence in the Shire's reliability and responsiveness – Impact perceptions of governance and operational capability – Lead to increased complaints or scrutiny if service disruptions are not effectively managed	Moderate (3)	Possible (3)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.