

Audit and Risk Committee - 21 September 2022 Attachments

6.1.1 AUDIT AND RISK COMMITTEE STANDING ITEMS SEPTEMBER

2022.....2

6.1.1.1 220916 AUDIT RECOMMENDATIONS PROGRESS REPORT

21092022.....2

6.1.1.2 ACTION ITEMS UPDATE 21092022.....7

6.1.2 FINANCE MANGEMENT REVIEW FY2022.....9

6.1.2.1 2022 CKB FINANCIAL MANAGEMENT REPORT.....9

6.1.3 OAG - LOCAL GOVERNMENT FOCUS REPORTS 2022.....22

6.1.3.1 FRAUD- RISK- MANAGEMENT- BETTER- PRACTICE- GUIDE.....22

6.1.3.2 INFORMATION- SYSTEMS- AUDIT- REPORT-2022- LOCAL-

GOVERNMENT- ENTITIES.....86

6.1.3.3 FINANCIAL- AUDIT- RESULTS- LOCAL-
GOVERNMENT-2020-21.....114

City of Kalgoorlie-Boulder

Objective

This report is to provide the audit committee with an update on the progress of actions taken by management to implement audit recommendations. The information is to help the audit committee monitor the timeliness of agreed actions and understand the reason for any delay.

Source and year	Report Date	Recommendation (record details)	Risk Rating	Manager responsible	Original completion date	Revised completion date	Status	Management Comments on action taken
Audit Findings 2019/20 – Grant Thornton/OAG	09/12/2020	Airport revenue supporting documentation – Recommend a documented review process be put in place to limit the risk of under reporting the number of passengers by the airlines	Moderate	David Trevaskis	June 2021	30/11/2022	Open	Airport has implemented a Conditions of Use Document over the Aerodrome, subject to commence July 2022. This document shall formalise the current informal arrangement and give the City audit capability over these metrics

<p>Audit Findings 2019/20 – Grant Thornton/OAG</p>	<p>09/12/2020</p>	<p>Documentation inconsistencies in IT policies – recommend management:</p> <ul style="list-style-type: none"> • Incorporate missing elements into existing documentation as listed • Finalise the implementation of formal policies where lacking and • Ensure that existing requirements be documented 	<p>Minor</p>	<p>Alyce Spokes</p>	<p>June 2021</p>	<p>30/11/2022</p>	<p>Open</p>	<p>Due to staff turnover during FY2021 this has been delayed. Policies will be updated during FY2022. (noted as a finding again 2021 audit)</p>
--	-------------------	---	--------------	---------------------	------------------	-------------------	-------------	---

<p>Audit Findings 2019/20 – Grant Thornton/OAG</p>	<p>30/04/2022</p>	<p>Disaster recovery plan - The City should ensure the DRP is adequately defined to meet these recovery requirements and tested on a regular basis. These tests should be used to confirm key IT systems and services can be restored or recovered within the required timeframes. The tests should also be used to verify that key staff are familiar with the plan and their specific roles and responsibilities in a disaster situation. The results of these tests should be documented, and relevant actions taken to improve the plan where necessary</p>	<p>Moderate</p>	<p>Alyce Spokes</p>	<p>30/06/2022</p>	<p>31/12/2022</p>	<p>Open</p>	<p>The City awarded a managed services contract to an external consultant in July 2021. Urgent works to address immediate shortcomings within the ICT environment were a priority. A full disaster recovery solution will be in place by June 2022. Currently all data and servers are backed up off site in Perth to ensure minimal loss to the business in the event of a disaster</p>
--	-------------------	---	-----------------	---------------------	-------------------	-------------------	-------------	--

<p>Audit Findings 2019/20 – Grant Thornton/OAG</p>	<p>30/04/2022</p>	<p>Cybersecurity testing - Management should perform tests to assess vulnerabilities of the IT environment on a periodic basis in order to identify potential vulnerabilities and improve the strength of IT security measures</p>	<p>Moderate</p>	<p>Alyce Spokes</p>	<p>31/12/2022</p>	<p>31/12/2022</p>	<p>Open</p>	<p>Since the audit was completed a Cyber Security process has been implemented, including social engineering fraud and threat testing. The City has run multiple threat tests in the last few months and have performed end user training to assist in mitigating end user risks. ICT are currently working to upgrade all ICT equipment, having already completed the main firewall upgrade and implemented 24x7 cyber security services to also mitigate this risk. All works aiming to be completed by December 2022</p>
--	-------------------	--	-----------------	---------------------	-------------------	-------------------	-------------	---

Financial Management Review June 2022 – Hall Chadwick	14/09/2022	Bank reconciliations and petty cash management – Bank, trust fund and petty cash reconciliations are recommended to be completed within 15 business days after month end.	Minor/low	Xandra Curnock	30/09/2022	30/09/2022	Resolved	Reconciliations to be completed as recommend.
Financial Management Review June 2022 – Hall Chadwick	14/09/2022	Credit card purchases – Recommend CKB to update its credit card policy to reflect updated processes (use of mobile phone app)	Moderate	Xandra Curnock	31/10/2022	31/10/2022	Open	Credit Card Policy to be reviewed and updated as recommended.

Resolution Register 2021							
OCM Meeting Date	Item No	Item Name	Author	Responsible Officer	Department	Council Resolution	Action Progress
23-Aug-21	14.2.3	INTEGRITY STRATEGY FOR WA PUBLIC AUTHORITIES 2020 -2023	David Trevaskis	John Walker	Deputy CEO	That Council: 1.Receive the Integrity Strategy for WA Public Authorities 2020 - 2023; and 2.Advise the CEO to complete the Integrity Snapshot Tool to help identify areas for development or more focus that should be included in the City's Risk Register.	1.Received - no further action 2. Integrity Snapshot Tool still to be completed
23-Aug-21	14.2.4	STRATEGIC RISK REGISTER	Eve Reitmajer	David Trevaskis	Deputy CEO	That Council: 1.Adopt the August 2021 Strategic Risk Register; and 2.Recommend the Finance and Audit Committee, once reconstituted after the election, consider the matter of the strategic risk register and the frequency of its review, with a view to: (a) Moving to a six (6) monthly review; and/or (b) Having an independent audit of the register carried out.	1.Received - no further action 2. (a) completed 2. (b) independent audit still to be completed
13-Dec-21	15.1.7	Name Change of the Committee & Committee Meeting Schedule 2022	Emma Holtum	David Trevaskis	Deputy CEO	That Council: 1.Change the name of the Finance and Audit Committee to the Audit and Risk Committee and update the Terms of Reference for this change. 2.Approve the following meeting dates for the Committee for the calendar year 2022: Wednesday 16 March 2022, Wednesday 15 June 2022, Wednesday 14 September 2022, Wednesday 7 December 2022.	1.Terms of Reference to be updated at OCM September 2022 2. Completed
13-Dec-21	15.1.8	Straetgic Risk Register	David Trevaskis	David Trevaskis	Deputy CEO	That Council: 1.Receives the November 2021 Strategic Risk Register as reviewed by the Committee. 2. Amend the City of KAlgoorlie-Boulder Finance and Audit Committee Work Plan to include 6 monthly review of the Strategic Risk Register. 3. Request the CEO to engage an independent consultant to conduct a review of the City's strategic risk register and submit recommendations to the committee for consideration.	1. no further action 2. completed 3. Hall Chadwick engaged to complete work. Report due end of September 2022

Resolution Register 2022							
OCM Meeting Date	Item No	Item Name	Author	Responsible Officer	Department	Council Resolution	Action Progress
28-Mar-22	14.2.1	Compliance Audit Return 2021	Emma Holtum	David Trevaskis	DCEO	That Council: 1. Receive and endorse the submission of the Compliance Audit Return for the period 1 January 2021 – 31 December 2021 to the Department of Local Government, Sport and Cultural Industries in accordance with the Local Government (Audit) Regulations 1996; and 2. Note the actions being undertaken as described in the report to address the issues identified in the Compliance Annual Return.	Complete
28-Mar-22	14.2.2	Financial Management Systems Review 2022	Xandra Curnock	David Trevaskis	DCEO	That Council: 1. Note the requirement for the financial management systems review to be compliant with regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 2. Approve the budget amendment of up to \$25,000 for an external consultant to perform the financial management systems review	Hall Chadwick has been engaged. Review commenced in June 2022. Report due end of September 2022
28-Mar-22	14.2.3	Altus Update - March 2022	Xandra Curnock	David Trevaskis	DCEO	That Council receive the update for the implementation of Altus Core Financials .	Complete
28-Mar-22	14.2.4	Audit and Risk Committee Standing Items March 2022	David Trevaskis	David Trevaskis	DCEO	That Council receive the information.	Complete
23-May-22	14.1.1	2020-21 Annual Financial Report	Xandra Curnock	David Trevaskis	DCEO	That Council: 1. Accepts the Annual Financial Report of the City of Kalgoorlie-Boulder and the accompanying Independent Audit Report for the financial year 2020. 2. Accepts the Auditors Management Report / Findings Report in respect of the financial audit for the financial year 2020-21.	Complete
25-Jul-22	14.1.1	Financial Management Systems Review 2022	Xandra Curnock	David Trevaskis	Directorate Corporate and Commercial	That Council accepts the update on the Finance Management Review for 2022	Complete
25-Jul-22	14.1.2	Audit and Risk Committee Standing Items June 2022	David Trevaskis	David Trevaskis	Directorate Corporate and Commercial	That Council receive the information.	Complete
25-Jul-22	14.1.3	Strategic Risk Register	David Trevaskis	David Trevaskis	Directorate Corporate and Commercial	That Council receives the June 2022 Strategic Risk Register as reviewed by the committee	Complete
25-Jul-22	14.1.4	Reserves at 30 June 2022	Xandra Curnock	David Trevaskis	Directorate Corporate and Commercial	That Council accepts the estimated reserve position at 30 June 2022	Complete
25-Jul-22	14.1.5	Update on loan borrowings	Xandra Curnock	David Trevaskis	Directorate Corporate and Commercial	That Council note the closing position of the loan borrowings at 30 June 2022	Complete



Financial Management Review

City of Kalgoorlie Boulder

June 2022

CONTENTS

1 Independent Reviewer’s Report 1
2 Executive Summary 3
3 Scope 5
4 Areas Examined with Findings, Observations and Recommendations 6
5 Disclaimer..... 9

1. INDEPENDENT REVIEWER'S REPORT

INDEPENDENT REVIEWER'S REPORT TO THE CHIEF EXECUTIVE OFFICER (CEO) OF THE CITY OF KALGOORLIE BOULDER

At the request of the CEO, Hall Chadwick Audit (WA) Pty Ltd was engaged to conduct a limited assurance review of the appropriateness and effectiveness of the City of Kalgoorlie Boulder's financial management systems and procedures. The objective of the review is to assist the CEO discharge responsibilities in respect to Regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 (as amended). The review was conducted for the period 1 July 2021 to 30 June 2022.

CEO's Responsibility for Maintaining and Reviewing Financial Management Systems and Procedures

The CEO is responsible for implementing policies, procedures and controls which are designed to ensure the effective and efficient management of the City's resources. In accordance with Regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 (as amended), the CEO is to undertake reviews of the appropriateness and effectiveness of the financial management systems and procedures. At least once in every four financial years the CEO is to report the results of those reviews to Council.

Our Responsibility

Our responsibility is to provide a report expressing limited assurance, designed to enhance the confidence of the CEO to assist reporting on the appropriateness and effectiveness of the financial management systems as required by Regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 (as amended). We conducted our engagement in accordance with Australian Standard on Assurance Engagements ASAE 3500 Performance Engagements issued by the Australian Auditing and Assurance Standards Board and the Audit Guidelines, in order to state whether, based on the procedures performed, anything has come to our attention that causes us to believe that the City's financial management systems have not been operating effectively. Our engagement provides limited assurance as defined in ASAE 3500.

Our objectives in our tender letter were agreed by the City on the 5th May 2022.

Limitations of Use

This report is made solely to the CEO of the City of Kalgoorlie Boulder for the purpose of reporting under Local Government (Financial Management) Regulation 5(2)(c). We disclaim any assumption of responsibility for any reliance on this report to any person other than the CEO of the City of Kalgoorlie Boulder, or for any purpose other than that for which it was prepared. We disclaim all liability to any other party for all costs, loss, damages, and liability that the other party might suffer or incur arising from or relating to or in any way connected with the contents of our report, the provision of our report to the other party, or the reliance on our report by the other party.



Inherent Limitations

A limited assurance engagement is substantially less in scope than a reasonable assurance engagement conducted in accordance with ASAE 3500 and consequently does not allow us to obtain assurance that we would become aware of all significant matters that might be identified in a reasonable assurance engagement. Accordingly, we will not express an opinion providing reasonable assurance.

We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and its responsibility to prevent and detect irregularities, including fraud. Accordingly, readers of our reports should not rely on the report to identify all potential instances of non-compliance which may occur.

Any projection of the evaluation of the level of compliance to future periods is subject to the risk that the systems may become inadequate because of changes in conditions, or that the degree of compliance with management procedures may deteriorate.

Independence

In conducting our engagement, we have complied with the independence requirements of the Australian professional accounting bodies.

Conclusion

Based on our work described in this report (which is not an audit), nothing has come to our attention to indicate the City of Kalgoorlie Boulder has not established and maintained, in all material respects, appropriate and effective financial management systems and procedures during the period covered by our review being 1 July 2021 to 30 June 2022.

For those aspects of the City of Kalgoorlie Boulder's Financial Management system and procedures which were assessed as having opportunities for improvement, our findings are summarised at Section 2 of this report and detailed observations and comments are within Section 4 of this report.

A handwritten signature in blue ink, appearing to read 'Hall Chadwick'.

HALL CHADWICK AUDIT (WA) PTY LTD
ABN: 42 163 529 682

A handwritten signature in blue ink, appearing to read 'Michael Hillgrove'.

MICHAEL HILLGROVE
Director

Dated this 14th of September 2022
Perth, Western Australia

2. EXECUTIVE SUMMARY

The objective of our engagement as outlined in our tender letter dated 5 May 2022 is to provide a report expressing limited assurance designed to enhance the confidence of the intended user (in this instance the CEO) in the performance of the control environment of the financial management system of the City of Kalgoorlie Boulder (administered by City staff being the Responsible Party) for which the intended user (CEO) is ultimately responsible in accordance with the Act and Regulations.

It includes the performance of assurance procedures designed to test the financial management system and report to the CEO on the appropriateness and effectiveness of the control environment within, as required by Financial Management Regulation 5(2)(c).

Summary of Results

The following is a summary of areas reviewed where nothing has come to our attention to indicate appropriate and effective financial management systems and procedures had not been established and maintained.

AREAS REVIEWED
<p>BANK RECONCILIATION AND PETTY CASH MANAGEMENT Internal controls over bank reconciliations and procedures are operating effectively.</p>
<p>TRUST FUNDS Trust funds adequately controlled and statutory requirements met.</p>
<p>RECEIPTS AND RECEIVABLES Internal controls over receipts and receivables are operating effectively.</p>
<p>FEES AND CHARGES Internal controls over fees and charges are operating effectively and statutory requirements were met.</p>
<p>PURCHASES, PAYMENTS AND PAYABLES (INCLUDING PURCHASE ORDERS) Internal controls over purchases and payables are operating effectively.</p>
<p>PAYROLL Internal controls over payroll are operating effectively.</p>
<p>CREDIT CARD PROCEDURES Internal controls over credit cards are operating effectively.</p>
<p>FIXED ASSETS Internal controls over fixed assets system and procedures are operating effectively.</p>
<p>MINUTES AND MEETINGS Procedures and protocols surrounding meetings and the quality of minutes of a satisfactory standard and in accordance with legislative requirements.</p>
<p>FINANCIAL REPORTS Financial Reports of a satisfactory standard and in compliance with legislative requirements.</p>
<p>BUDGET The adopted budget was of satisfactory form and content and met all statutory requirements.</p>
<p>DELEGATIONS The delegations register complies with statutory requirements.</p>
<p>AUDIT COMMITTEE The audit committee complies with statutory requirements.</p>
<p>INSURANCE Insurance up to date and reviewed annually.</p>
<p>STORAGE OF DOCUMENTS/RECORD KEEPING Records management systems are operating effectively.</p>
<p>GENERAL COMPLIANCE AND OTHER MATTERS Internal controls and restrictions over general journal entries and investments maintained properly. IT general environment considered appropriate for the City's needs.</p>

2. EXECUTIVE SUMMARY

Recommendations

As referred to in Section 1, a brief summary of our findings identified are as follows:

FINDINGS	RATING
<p>CREDIT CARD PROCEDURES</p> <ul style="list-style-type: none"> The policy needs to be updated to reflect the current procedures performed 	Moderate
<p>BANK RECONCILIATIONS</p> <ul style="list-style-type: none"> All Cash and Trust Reconciliations must be performed in a timely manner 	Low

The findings are given a risk rating as an indication of the potential risk if not satisfactorily resolved.

Risk Level	Action Required
Very High	Senior management attention needed and should have a very high priority for immediate action. Immediate action is generally required.
High	Senior management attention needed and should have a high priority for immediate action. Immediate action is generally required.
Moderate	Management responsibility and timeframe for risk reduction must be specified. Corrective action is generally required as soon as possible.
Low	Manage by routine procedures – action when resources permit. Corrective action is required but with a lower priority than higher risks.

Further details are in Section 4 of this report, including our recommendations to assist the City in maintaining an appropriate and effective financial management systems and procedures.

Conclusion

Based on our work performed, nothing has come to our attention to indicate that the City has not established and maintained, in all material respects, appropriate and effective financial management systems and procedures during the period covered by our review being 1 July 2021 to 30 June 2022.

3. SCOPE

Scope

Our review covered the period 1 July 2021 to 30 June 2022 and encompass the following financial systems and procedures of the City:

- Purchases, Payments and Payables (Including Purchase Orders)
- Receipts/Receivables
- Payroll
- Rates
- Bank Reconciliations
- Trust Fund
- Fees and Charges
- Minutes and Meetings
- Financial Reports
- Budget
- Plan for the Future
- Fixed Assets
- Delegations
- Registers
- Audit Committee
- Insurance
- Storage of Documents/Record Keeping
- Credit Card Procedures
- General Compliance and Other Matters

Our review did not cover any provisions of the Act or Regulations which were non-financial in nature.

4. AREAS EXAMINED WITH FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

4.1 Bank Reconciliations and Petty Cash Management

Bank Reconciliations

Reviews of bank reconciliations and procedures for the agreed period were performed with the following observations noted:

Findings / Observations	Recommendations
HC randomly selected two months of bank reconciliations and noted an instance where bank reconciliation was prepared after 15 business days.	Bank reconciliations are recommended to be completed within 15 business days after month end.
HC randomly selected two months of bank reconciliations and noted three instances where outstanding deposits and unrepresented cheques standing stale for more than a month.	Outstanding deposits and unrepresented cheques are recommended to be follow up after a month.

Trust Funds

Reviews of trust fund bank reconciliations and procedures for the agreed period were performed with the following observations noted:

Findings / Observations	Recommendations
10 months of bank reconciliations are reviewed and there are 9 instances where the bank reconciliations are not prepared promptly.	Trust fund reconciliations are recommended to be completed within 15 business days after month end.

Petty Cash Management

Reviews of trust fund bank reconciliations and procedures for the agreed period were performed with the following observations noted:

Findings / Observations	Recommendations
HC randomly selected three months of petty cash reconciliations and noted two instances in GOA reconciliation were signed but not dated; and noted one instance in Admin reconciliation were performed before month end.	Petty Cash reconciliation are recommended to be completed within 15 business days after month end.

4.2 Receipts and Receivables

Review of the receipts and receivables process and procedures, together with randomly selected receipt samples for the agreed period were performed without any weaknesses/observations noted.

4.3 Rates

Review of the rating procedures, including inspection of the rate notices, instalment notices and valuation reconciliation were performed, together with testing of randomly selected samples for the agreed period. There were no weaknesses/observations noted.

4.4 Fees and Charges

Review of the fees and charges procedures, including allocations were performed, together with testing of randomly selected samples for the agreed period. There were no weaknesses/observations noted.

4. AREAS EXAMINED WITH FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

4.5 Purchases, Payments and Payables (including Purchase Orders)

A sample of 15 payment transactions were randomly selected and tested to determine whether purchases were authorized, budgeted and payments were supported, and correctly allocated. The City’s purchases, payments and payables system was also examined to determine if adequate controls were in place in ensuring liabilities are properly recorded and payments are properly controlled.

In general, controls and procedures over payments and payables are operating effectively and are appropriate for the City’s current scope of operations, with the following exceptions being assessed as having the opportunity for improvement:

Findings / Observations	Recommendations
We noted that for purchase above tender threshold, regularly used suppliers would become part of the City’s list of preferred suppliers on VendorPanel and all suppliers are free to apply to be invited to VendorPanel. Evaluation process only starts at the evaluation of quotes.	Every expense area ranging from expenses below tender threshold to above tender threshold should have a preferred supplier list taking into account the price, quality of goods & services. Evaluation of supplier should happen when supplier applied to become preferred supplier on VendorPanel to ensure all suppliers on preferred supplier listing are of high quality.
Noted three instances where proforma invoices dated after actual invoice; one instance where purchase order dater after invoice; four instances where invoice received before requisition occur.	The purchase procedure of Budget > Quote/Tender > Requisition > Purchase Order > Invoice should be followed to ensure every purchase are well budgeted for.

4.6 Payroll

A random sample of 15 individual employees was selected from one randomly selected pay run and for each employee’s pay, the following testing was performed to help ensure:

- the employee existed;
- the correct rate of pay was used;
- non-statutory deduction authorities are on hand;
- time sheets were properly completed and authorised;
- hours worked were properly authorised; and
- allocations were reasonable and correctly posted.

We also tested the first pay of two new employees and the last pay of two terminating employees (randomly selected) from the same pay run.

The City’s payroll system was also reviewed to determine if adequate controls were in place to help ensure wages and salaries were properly processed and payments are properly controlled.

The system described to us and its supporting controls were found to be operating effectively, except for the following:

Findings / Observations	Recommendations
We noted there is no notification given to employees in regard to a pay rise resulting from awards adjustment as per EBA. Awards are adjusted as per EBA from the first pay period after date specified in EBA. There is an instance where we couldn’t match the pay rate as per employment contract to pay rate as per payslips due to this increment from EBA, as no further supporting documents were issued to the employee since the first contract.	Though increment from EBA may be fixed from the beginning of the employment, it is recommended that CKB issue a notification letter to the relevant employee advising the pay rate change on the effective date. This ensure pay rate changes are captured.

4. AREAS EXAMINED WITH FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

Salaries and wages are compared to budget as a whole and was performed monthly.	It is recommended that the comparison to be done for each department so better cost control can be implemented.
Long service leave information is not held in Definitiv, and spreadsheet is prepared yearly to account for LSL eligibility.	Long service leave reconciliation should be done every month to capture errors timely.

4.7 Credit Card Procedures

A review of the City’s credit card procedures was performed to determine if adequate controls were in place.

26 credit cards are currently in use. We randomly selected 10 credit card transactions across the cards to determine whether they are legitimate and usual in the context of the City’s operations. This included:

- sighting tax invoices;
- ascertaining whether the transaction is for bona fide City business;
- ensuring the purchase is budgeted for;
- determining whether transactions are in line with the City’s policy; and
- determining whether the credit card reconciliation and reporting are carried out as per the City’s credit card policy.

Upon review, the following observations noted:

Findings / Observations	Recommendations
<p>As per the City’s credit card policy, as part of the process for credit card reconciliation and reporting, the cardholder sign and date the credit card statement with supporting documentation attached stating 'all expenditure is of business nature'. In our findings, CKB have moved to an electronic coding system and no longer have manual approvals of statements.</p> <p>As per the City’s credit card policy, the allocation of the credit card was approved by the CEO & copy of the credit card application form signed by the cardholder and two signatories to the City’s bank account. In our findings, CKB mentioned they don’t require two signatories on the bank account for the credit card application. They require their manager, General Manager and CEO approval.</p> <p>Credit card policy is not up to date with all the changes taken place.</p>	<p>Recommend CKB to update its credit card policy to reflect the updated process.</p>

4.8 Fixed Assets

Review of the fixed assets procedures, including controls over acquisition and disposal of assets, updating of the fixed assets register and reconciliation of the fixed assets register to the general ledger, together with selected depreciation samples for the agreed period were performed. There were no weaknesses/observations noted.

4. AREAS EXAMINED WITH FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

4.9 Minutes and Meetings

Council and Committee meeting minutes were reviewed to ensure compliance with procedures and protocols with no weaknesses/observations noted.

4.10 Financial Reports

The previous period annual report for the 2021 Financial year (including financial report) and monthly financial reports were reviewed for compliance with legislative requirements with no weaknesses/observations noted. At the time of producing this report, the financial report for the current period 2022 has not been finalised thus we have relied on the prior year's report.

4.11 Budget

We obtained an understanding of the budget process without any weaknesses/observations noted.

4.12 Plan for the Future

The City currently has in place the Long-Term Financial Plan (2020 – 2030), Strategic Community Plan (2020-2030) and Corporate Business Plan (2021 – 2024). From examination, all plans appear to meet all statutory requirements and no issues are noted.

4.13 Registers

From our reviews of all Registers, we are satisfied that they meet all regulatory requirements, no other matters were noted.

4.14 Delegations

From our reviews performed on the areas of scope, in relation to the delegation of duties, no matters were noted.

4.15 Audit Committee

The City's establishment of its audit committee and the constituted membership was examined as well as the review of all committee minutes during the period. No concerns noted.

4.16 Insurance

No matters were noted from our discussions with management and review of insurance policy documents. Insurance policies are purchased and updated annually.

4.17 Storage of Documents / Record Keeping

We note that the City follows their Record Keeping Policy which includes online storage or all documentation as well as physical archived storage. No matters were noted from our discussions with management.

4. AREAS EXAMINED WITH FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

4.18 General Compliance and Other Matters

Investments

Internal control procedures and restrictions over investments are properly maintained and complied with the Local Government (Financial Management) Regulation.

General Journals

Internal control procedures over general journals are properly maintained for the level of operations.

IT General Environment

We have obtained an understanding of the City's IT general environment, including general controls such as access to the computer system, regular changes to passwords and data back-up. An IT Disaster recovery test occurred with no incidents occurring, thus we are satisfied.

5. DISCLAIMER

The objective of this review as outlined Section 1 of this report as presented, is to assist the Chief Executive Officer of the City of Kalgoorlie Boulder discharge responsibilities in respect to Regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 (as amended).

It has been prepared by Hall Chadwick Audit (WA) Pty Ltd for this sole purpose. It is not intended to be used by any other individual or organisation.

Confidential – this document and the information contained in it are confidential and should not be used or disclosed in any way without our prior consent.

**Office of the Auditor General
Western Australia**

Report team:

Carl Huxtable
Chiara Galbraith

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.

© 2022 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Fraud Risk Management
– Better Practice Guide**

Report 20: 2021-22
June 2022

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

FRAUD RISK MANAGEMENT – BETTER PRACTICE GUIDE

This report has been prepared for submission to Parliament under the provisions of section 23(2) and 24(1) of the *Auditor General Act 2006*.

Better practice checklists regularly feature in my Office's performance audit reports as a means of providing guidance to help the Western Australian public sector perform efficiently and effectively. This is the third comprehensive stand-alone better practice guide we have produced.

A handwritten signature in black ink, appearing to read 'Caroline Spencer'.

CAROLINE SPENCER
AUDITOR GENERAL
22 June 2022

Contents

Auditor General's overview.....	2
Part 1: Introduction	3
1.1 About this guide.....	3
1.2 Who should use this guide	3
1.3 What is fraud and corruption.....	3
1.4 Fraud control principles	4
1.5 Acknowledgements	5
Part 2: Why develop a fraud risk management program	6
2.1 Overview	6
2.2 Public sector requirements	6
2.3 Impact of fraud in the WA public sector	6
2.4 Status of fraud control maturity across the sector	8
Part 3: How to develop a fraud risk management program	10
3.1 Overview	10
3.2 Where to look for fraud vulnerabilities.....	11
3.3 Fraud risk management process	12
Appendix 1: Glossary	25
Appendix 2: References	27
Appendix 3: Fraud control system benchmarking tool	28
Appendix 4: External threat assessment tool.....	32
Appendix 5: Tools to support the fraud risk management process	37
A5.1 Communication and consultation tool.....	37
A5.2 Scope context and criteria tool	38
A5.3 Risk assessment tools	39
A5.4 Risk treatment tools	50

Auditor General's overview

Fraud and corruption are ever present and growing threats to businesses, including the Western Australian public sector. As well as loss of funds, fraud and corruption can result in loss of confidence in government institutions. The community needs to have faith that the public sector is serving them well for democracy to work.



The social contract between taxpayer and Government is threatened when public money is misappropriated or other wrongdoing occurs. It strikes at the core of trust, accountability and transparency in Government.

Good governance is important to protect our power, water, justice and transport infrastructure, as well as our health, education and regulatory systems from ineffectiveness, inefficiency and of course failure to deliver what people need when they need it.

It is therefore critical that all levels of the Western Australian (WA) public sector commit to good governance to safeguard public assets from fraudulent or corrupt activity. To do this, every WA public sector entity must understand, in detail, the risks that occur generally within the public sector environment and the specific risks relevant to the activities they undertake.

A common motivator for most people who join the public sector is a desire to do a good job. To assist with this we develop and share guidance on better practice. The purpose of this Better Practice guide is to raise the standard of fraud and corruption control across the WA public sector. Parts 1 and 2 of this guide are aimed at decision makers, highlighting the importance of a fraud and corruption risk management program and the current state of fraud control in the WA public sector. Part 3 is aimed at guiding those responsible for developing and implementing an entity's fraud risk management program.

The guide follows the establishment of our Forensic Audit team as set out in my report of December 2021, its purpose being to uplift fraud resilience within the WA public sector. As has always been the case, public sector entities are responsible for the prevention and detection of fraud and corruption. This guide is intended to empower entities to do more to discharge their governance responsibilities by better controlling their risks of fraud and corruption.

We encourage entities to use this guide along with the tools and other available resources to manage the risk of fraud against their entity. While fraud risks cannot be eliminated, a robust and well-resourced fraud risk management program can minimise the likelihood and consequences of fraud events.

We thank the Commonwealth Fraud Prevention Centre for their generous support in helping develop this guide as well as McGrathNicol Advisory for their guidance. We also extend our appreciation to the State entities that provided valuable feedback on the draft guide.

Part 1: Introduction

1.1 About this guide

This Better Practice Guide aims to help Western Australian (WA) public sector entities to manage their fraud and corruption risks. It outlines why fraud and corruption risk management is important (Part 2) and provides practical guidance on the process of developing a fraud and corruption risk management program (Part 3).

The guide refers to a range of tools which are included in the appendices and available on our website (www.audit.wa.gov.au). The online tools will be updated as required.

1.2 Who should use this guide

This guide is intended for use by WA public sector entities (entities) and may be applicable to other organisations.

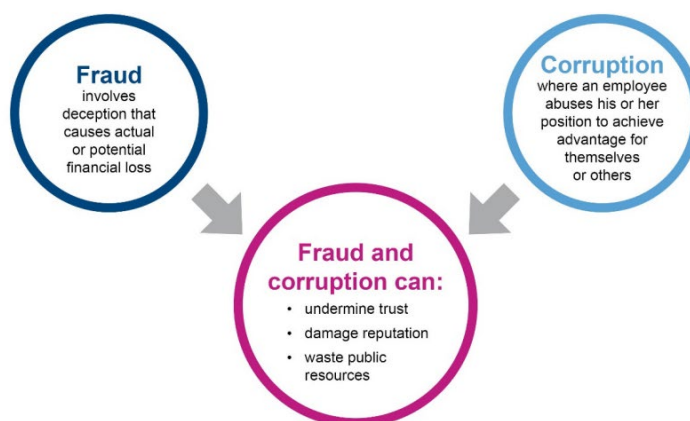
Parts 1 and 2 are intended for directors general, chief executive officers, managers and other key decision makers. Part 1 outlines the high-level principles entities should apply to fraud and corruption risk management and Part 2 highlights the importance of entities implementing an effective fraud and corruption risk management program.

Part 3 is for those tasked with fraud risk management within an entity. It aims to step them through the process of developing, executing and monitoring an entity’s fraud and corruption risk management program.

Ultimately, preventing and detecting fraud and corruption is the responsibility of every person in the WA public sector, and as such, this guide may be relevant for all public sector employees.

1.3 What is fraud and corruption

Fraud and corruption involve a benefit being obtained through dishonesty and/or an abuse of position to the detriment of another person or entity (Figure 1). They can pose a risk to an entity’s finances, reputation, and service delivery. More seriously, they go to the heart of trust and confidence in Government. In this guide, we use the term fraud to include corruption.



Source: OAG using information from the Victorian Auditor General’s Office – *Fraud and Corruption Control* report, March 2018

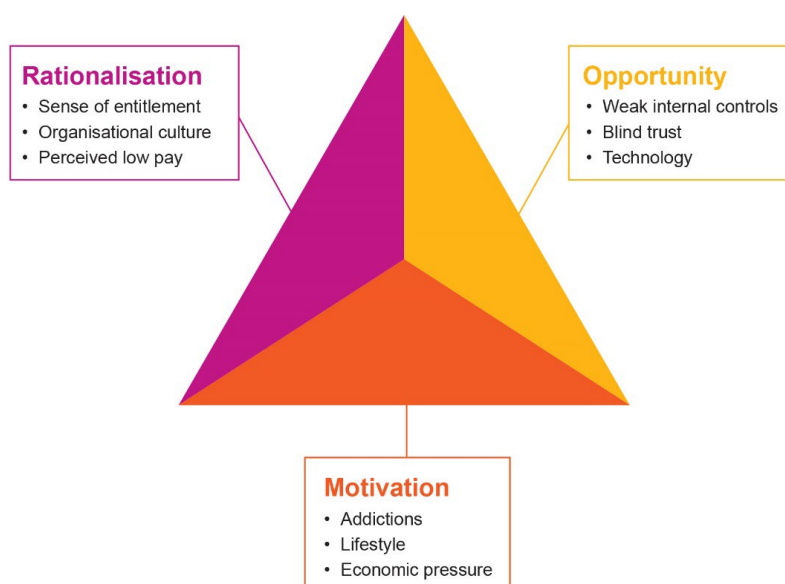
Figure 1: Definitions of fraud and corruption

Not all fraud can be prevented – every organisation, public or private, is vulnerable. A robust and rigorous fraud control system, with appropriate prevention and detection processes, can reduce the risk of fraud occurring and minimise losses.

To effectively fight fraud an entity must first acknowledge that fraud occurs and then seek to understand how and why it occurs. The fraud triangle (Figure 2) outlines 3 key elements that are generally present when fraud has occurred in an entity:

- **Opportunity** – a vulnerability within systems or processes is identified and exploited.
- **Motivation** – also referred to as pressure, is the reason someone commits fraud.
- **Rationalisation** – how someone justifies their fraudulent behaviour to themselves.

With the right mix of motivation, opportunity and rationalisation even the most trusted employee can be tempted to commit a fraudulent act.



Source: OAG adapted from Other People's Money¹

Figure 2: The fraud triangle

A fraudster's personal motivation and the ability to rationalise their behaviour is largely beyond an entity's control although, entities will benefit from being alert to and aware of behavioural red flags in respect of their staff and suppliers. The most effective way for an entity to manage its risk of fraud is by controlling the opportunity – implementing or enhancing controls aimed at preventing fraud or detecting it quickly if it does occur.

1.4 Fraud control principles

To build a robust and effective fraud risk management program requires 10 essential principles. Each of the following principles link to 1 or more stages of a better practice fraud risk management program as set out in this guide.

¹ *Other People's Money: A Study in the Social Psychology of Embezzlement*, Dr Donald Cressey, Free Press 1953.

Strong leadership	An entity's leadership must model a commitment to fraud control, establishing a strong 'tone at the top' culture to demonstrate their personal commitment to operating with integrity and encouraging a 'finding fraud is good' mindset.
Recognise fraud as a business risk	Entities must acknowledge they are vulnerable to fraud. Fraud should be viewed and treated in the same way as an entity's other enterprise risks.
Adequate control resourcing	Entities should invest in appropriate levels of fraud control resourcing including specialist information system security management personnel.
Clear accountability for fraud control	Entities should establish clear personal accountabilities for fraud control at the governance, executive management and management levels.
Implement and maintain an effective fraud control system	An effective fraud control system (FCS) can reduce the opportunity for fraud. It needs to align with better practice guidance, be fully implemented, monitored and updated periodically.
Periodic assessment of fraud risks	Fraud risk assessments should be carried out periodically or whenever a significant change that affects the entity occurs.
Effective awareness raising program across the entity	To ensure employees recognise red flags for fraud, entities should establish an effective awareness program.
Open channels to report suspicions of fraud	To encourage whistle-blowers to come forward entities should support: <ul style="list-style-type: none"> • active reporting of fraud through accessible anonymised reporting channels • ensure that the entire workforce is aware of organisational expectations for reporting detected or suspected cases of fraud • ensure they have robust whistle-blower protection policies and procedure that includes assurance that victimisation of those who, in good faith, make such reports will not be tolerated.
Implement a fraud detection program	An effective fraud detection program that includes detection measures such as data analytics and post-transactional review are important.
Consistent response to fraud incidents	Rapid and robust response to suspected fraud events with effective investigation procedures will drive decisive action and result in better outcomes for detected fraud incidents. A strong and consistent response to all fraud events will send a strong message to the workforce that the entity will not tolerate fraud, no matter how minor.

Source: OAG

Table 1: Foundation principles for fraud control

1.5 Acknowledgements

We would like to express our appreciation to the entities and their employees who contributed to the development of this guide.

We also acknowledge and express our appreciation to the Commonwealth Fraud Prevention Centre (CFPC) and Standards Australia, who willingly shared their original intellectual property in the development of this guide, and McGrathNicol Advisory, who were engaged to provide technical expertise.

Part 2: Why develop a fraud risk management program

2.1 Overview

In this part of the guide, we outline why entities should develop a fit for purpose fraud risk management program. In summary:

- there are WA government requirements to implement integrity measures to protect the financial and reputational position of entities
- the financial, reputational and human impact on an entity and its employees when fraud occurs can be significant
- entities' fraud control maturity is not meeting best practice.

Fraud risk management has a critical role in preventing and promptly detecting fraud to minimise loss, retain trust in entities and protect employees.

2.2 Public sector requirements

Entities are required to consider their risks and implement protections.

Treasurer's Instruction (TI) 825 requires all WA State government entities to develop and implement a risk management program. The TIs state, where possible, entities' policies and procedures should be consistent with Australian Standards including:

- AS ISO 31000:2018 – *Risk management - Guidelines* (risk standard)
- AS 8001:2021 – *Fraud and corruption control* (fraud control standard).

Similarly, Regulation 17 of the Local Government (Audit) Regulations 1996 requires local government CEOs to review their entity's systems and procedures, including for risk management, to ensure they are effective and appropriate for the entity's needs.

In addition to these requirements, the Public Sector Commission encourages all entities to commit to implementing its *Integrity Strategy for WA Public Authorities 2020-2023*. This strategy includes the *Integrity Snapshot Tool* which enables entities to self-assess their current integrity position and help identify areas for improvement.

This guide is intended to aid all entities in the application of the above Australian Standards and is not a replication of them. Entities should obtain a copy of the above from Standards Australia or from an authorised distributor to ensure a full and proper understanding of the content and their compliance with them.²

2.3 Impact of fraud in the WA public sector

The Association of Certified Fraud Examiners Report to the Nations 2022, estimated that fraud losses in businesses, government and not-for-profits are approximately 5% of their

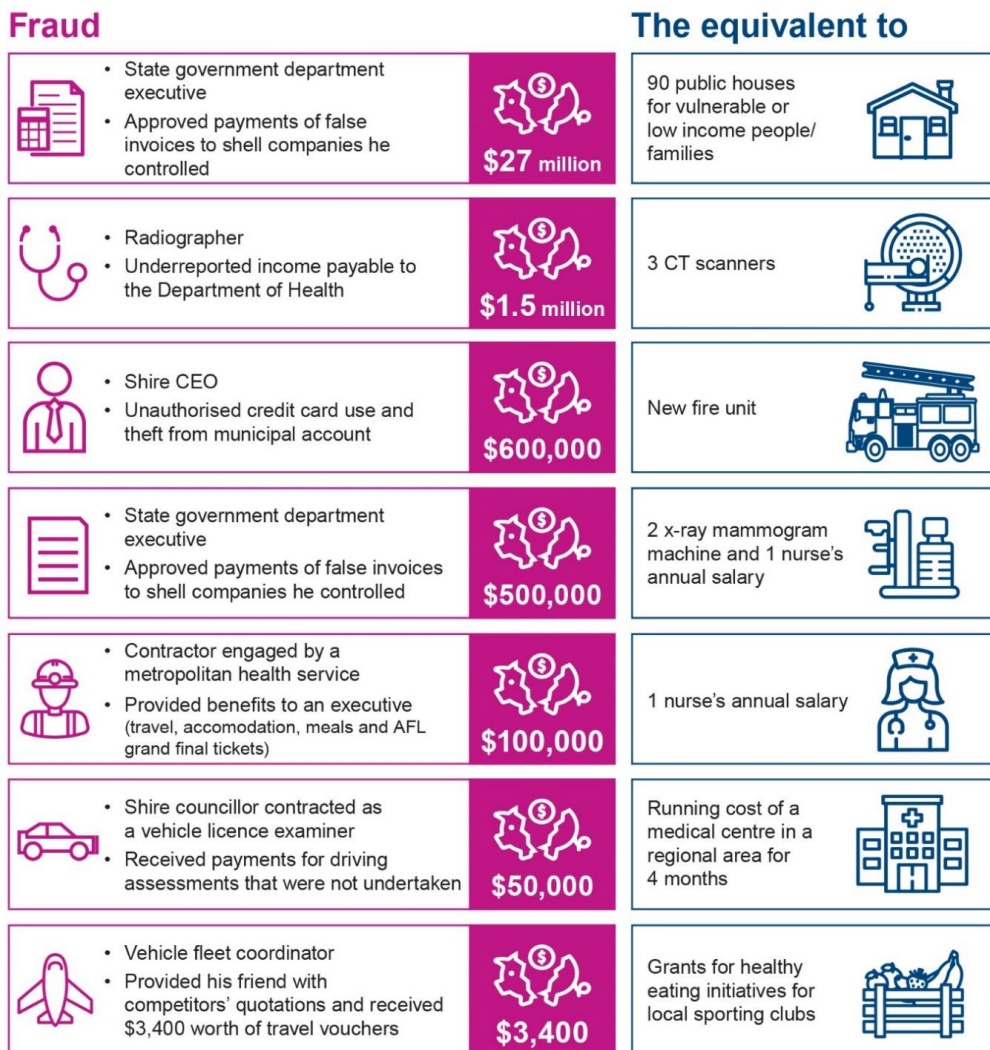
² Reproduced by Office of the Auditor General (WA) with the permission of Standards Australia Limited under licence CLF0622OAGWA.

Copyright in AS 8001:2021 and AS ISO 31000:2018 vests in Standards Australia and ISO. Users must not copy or reuse this work without the permission of Standards Australia or the copyright owner.

annual turnover.³ If this estimate is an accurate reflection of actual fraud losses within the WA public sector, the impact on the people of WA, and the services to them, is considerable.

Fraud within the WA public sector is typical of instances in other jurisdictions and sectors where investigations regularly find deficiencies within entities' controls. These deficiencies may have been identified earlier if the entities had a robust and rigorous fraud risk management program in place.

The following is a short summary of some detected fraud events within the WA public sector in the last 15 years and the practical impact on service delivery. These incidents demonstrate that the WA public sector remains vulnerable to fraud by members of its own workforce as well as external fraudsters.



Source: OAG

Figure 3: Examples of known fraud in the WA public sector

³ Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*.

The impact of fraud goes beyond financial and service delivery losses and includes:

- **Human impact:** Those who rely on government services (such as the elderly, the vulnerable, the sick and the disadvantaged) are often the ones most harmed by fraud, increasing the disadvantage, vulnerability and inequality they suffer.
- **Reputational impact:** When it is handled poorly, fraud can result in an erosion of trust in government and industries, and lead to a loss of international and economic reputation. This is particularly true when fraud is facilitated by corruption.
- **Industry impact:** Fraud can result in distorted markets where fraudsters obtain a competitive advantage and drive out legitimate businesses, affecting services delivered by businesses and exposing other sectors to further instances of fraud.
- **Environmental impact:** Fraud can lead to immediate and long-term environmental damage through pollution and damaged ecosystems and biodiversity. It can also result in significant clean-up costs.⁴
- **Organisational impact:** The impact of fraud on employees can be significant. It can lead to low morale, mistrust, inefficient additional oversight and ultimately staff leaving due to the entity’s damaged reputation. It can also result in reduced efficiency and effectiveness of the entity’s activities.

2.4 Status of fraud control maturity across the sector

In 2021, we conducted a high-level review of State government entities’ fraud risk management. As reported in our *Forensics Audit Report – Establishment Phase*, we found many entities fell well short of better practice. We reported similar results in our 2013 report, *Fraud Prevention and Detection in the Public Sector*, and in our 2019 report, *Fraud Prevention in Local Government*. Significant work is required across the public sector to raise the standard of fraud risk management to a satisfactory level.

As part of our 2021 review we asked: “Has the entity completed an assessment of its fraud and corruption risks?” Set out at Table 2 is an analysis of the findings of that review.

Responses			
Assessment completed	Assessment in progress	Assessment not completed	Total
71	12	11	92

Source: OAG

Table 2: Number of entities who have completed an assessment of their fraud and corruption risks

We selected a sample of 12 entities for more detailed analysis. This further analysis highlighted several key themes as set out in Table 3 below:

Theme	Summary	Why it matters
Lack of a risk framework	Some entities did not have an overall risk framework that could be applied in the context of fraud risk.	An overall risk framework ensures consistency in approach to all the entity’s identified risks.

⁴ [Commonwealth Fraud Prevention Centre, *The total impacts of fraud*](#) (accessed 17 May 2022).

Theme	Summary	Why it matters
Entity size not an indicator of quality	Several larger entities provided insufficient details to show they had undertaken a fraud risk assessment. This suggests that inadequate resourcing is not the sole cause of poor fraud risk assessments being conducted.	The public sector collectively provides a diverse range of services and entities should apply a fit for purpose approach to their fraud risk assessment.
Lack of collaboration	Our analysis suggested a lack of collaboration with risk and process owners in the identification and analysis of the entity's fraud risks.	Collaboration is important because different employees bring different perspectives and experience.
No fraud risk register	Many entities did not have a fraud risk register, despite this being a requirement of their fraud control program.	Entities cannot efficiently monitor and review fraud risks if they have not been documented. The appropriate way to document an entity's fraud risks is in a fraud risk register.
Failure to assess fraud risk	It was clear from our analysis that a significant proportion of entities had not assessed their fraud risks. In many cases entities mistook a fraud control framework for a fraud risk assessment.	Entities must ensure they have a sound understanding of fraud risks that could impact their organisation – this can only be done by implementing a comprehensive process to identify, analyse and evaluate specific fraud risks that could impact the entity.
Data analytics not targeted	Entities had not identified and assessed relevant fraud risks prior to undertaking data analytics to identify fraudulent transactions.	Data analytics is a useful tool for the prevention and detection of fraud, but it requires discipline for it to be efficient and effective. Entities risk implementing inefficient and costly data analytics that are not effective for fraud risks specific to their entity.
Excessive generalisation	Fraud risks that were identified were excessively general rather than being linked to specific processes.	Entities must properly identify and define their vulnerabilities to enable implementation of effective controls.
Risk register limited to strategic risks	Fraud had been identified as an overall strategic risk; however, we saw little evidence that specific fraud risks were identified for individual business units or that a comprehensive fraud risk assessment had been undertaken across all parts of the organisation.	

Source: OAG

Table 3: Themes identified from survey of entities' fraud control maturity

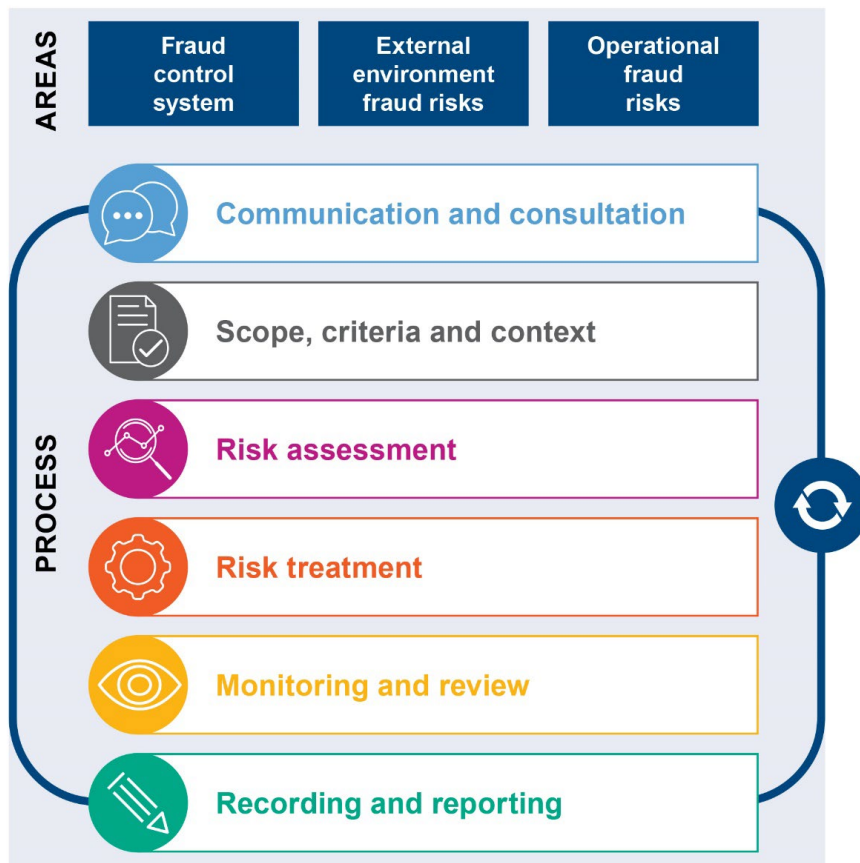
Part 3: How to develop a fraud risk management program

3.1 Overview

To effectively manage fraud risks, entities should develop and implement a robust and effective fraud risk management program. The program should be tailored to an entity’s objectives, environment and risk profile and cover:

- the 3 areas where fraud vulnerabilities can be found (based on AS 8001:2021 – *Fraud and corruption control*) – section 3.2
- the 6-stage process to manage risks (based on AS ISO 31000:2018 *Risk management – Guidelines*) – section 3.3.

The diagram below is a simple illustration of the fraud risk management program.



Source: OAG based on AS 8001:2021 and AS ISO 31000:2018

Figure 4: Risk management process including 3 areas of fraud risks to consider

3.2 Where to look for fraud vulnerabilities

In accordance with AS 8001:2021, effective management of fraud risk requires a comprehensive examination of an entity’s overall fraud control system (FCS), external threats and operational (or internal) activities.

Our survey of State government entities found that most entities who had taken steps to manage their risk of fraud only considered 1 of the 3 vulnerability areas and none provided evidence that they had considered all 3.

The following is a brief overview of the 3 areas of fraud vulnerability. Whilst we have focused the fraud risk management process that follows at 3.3 on operational risks, it can be applied to the other 2 areas of fraud vulnerability.

A fraud control system is the tools and techniques used to mitigate an entity’s fraud risks. When considering fraud risks, analysing the existing control environment is important to assess how closely it aligns to better practice.

AS 8001:2021 – *Fraud and corruption Control* Clause 2.10 identifies 4 elements for an FCS: foundation, prevention, detection and response, examples of these are included in the table below:

FCS elements	Overview
Foundation	Adequate resourcing to implement a multi-faceted approach to managing fraud risks. Examples include specialist resourcing, awareness training, risk management, information security management systems.
Prevention	Prevention controls are the most common and cost-effective way to mitigate fraud. Examples include an integrity framework, internal controls, workforce screening, physical security.
Detection	Detection controls can help to identify when fraud has occurred but are not as cost-effective as preventative measures. Examples include post-transactional review, data analytics, whistle-blower management.
Response	Response controls can assist the entity to respond to a fraud incident after it has occurred and are the least cost-effective, however can significantly reduce the impact of present and future frauds. Examples include investigation, disciplinary procedures, crisis management, recovery.

Source: OAG based on AS 8001:2021 – *Fraud and corruption control* Clause 2.10

Table 4: Elements of a fraud control system

Entities may not have formally documented their FCS, but it is likely they have several existing controls.

Designing and implementing a robust fraud risk management program will inevitably strengthen an entity’s FCS. It is for this reason it is recommended an entity assess their FCS against better practice prior to undertaking the fraud risk management process.

The fraud control standard (Clause 2.10) sets out an approach to developing and implementing an entity’s FCS and a structure for documenting it. Appendix 3 is a tool for entities to benchmark their current FCS maturity against the fraud control standard.

Updating the fraud control system documents throughout the fraud risk management process assists entities to monitor their increased maturity.

External threats come from outside an entity and are largely beyond their control. The fraud control standard recommends entities consider the 6 external factors that can impact an organisation, known as the PESTLE model. The model is explained in the table below and a complete tool is provided in Appendix 4:

PESTLE factor	Overview
Political	To identify the political situation of the country, State or local government area in which the entity operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and local, regional, national or international political pressure.
Economic	To determine the economic factors that could have an impact on the entity including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.
Social	To identify the expectations of society by analysing factors such as consumer demographics, significant world events, integrity issues, cultural, ethnic and religious factors, and consumer opinions.
Technological	To identify how technology, including technological advancements, social media platforms and the role of the internet more broadly, is affecting or could affect the entity.
Legal	To identify how specific legislation, including industry specific regulations, and case law are affecting or could affect the entity's future operations.
Environmental	To identify how national and international environmental issues are affecting or could affect the entity.

Source: OAG based on AS 8001:2021 – *Fraud and corruption control*, Clause 2.9

Table 5: External factors that can impact an entity

Operational fraud risks are the fraud risks associated with an entity's day-to-day operations. There will be risks that are common to all entities (e.g. procurement, payroll, asset management) and those that are entity specific (e.g. property development, grant administration, major projects). Operational risks will also include changes in function or activity (e.g. new government initiative, creation of a relief fund in response to a natural disaster). The following section, Fraud risk management process, is focused on managing your operational fraud risks and discusses this in more detail. We also provide further tools in the appendix to assist with better managing them.

3.3 Fraud risk management process

In this section we have mapped out the 6 stages in the risk management process as summarised in Figure 4 above. It is not a linear process; each stage will connect to others at different times throughout the risk management cycle.

We describe the stages and introduce several tools which can be used to assist in developing an effective fraud risk management program. The complete tools are included in the appendices and are available on our website. These tools are not an exhaustive list, there are many tools available (free and for a fee) and entities should determine which ones best suit their needs.

Communication and consultation

To effectively identify fraud risks within an entity’s processes and systems, it is essential that the people who best know and run or control the business processes and business area are adequately engaged throughout the fraud risk management process. Entities should also consider if subject matter experts need to be engaged, such as information system security specialists.



Communication and consultation are intended:
“...to assist stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.”⁵

Employees can feel challenged when asked to respond to questions or contribute to discussions about fraud risks – they may feel that considering this issue with them or in their presence is, in effect, calling their integrity into question. Those tasked with the fraud risk management program should keep the people they need engaged and at ease throughout the process to ensure the best outcome.

Communication and consultation	Better practice
Promote awareness and understanding of fraud risks	<ul style="list-style-type: none"> • Implement multimodal training programs specific to fraud risks – “What is a fraud risk” • Effectively communicate to employees that the objective is to protect the integrity of the entity and employees
Bring different expertise together throughout the process using effective mechanisms	<ul style="list-style-type: none"> • Engage different levels of expertise and experience to bring various perspectives • Use a variety of communication methods such as emails, workshops, one-on-one interviews and surveys to obtain a wide range of feedback and opinions
Build a sense of inclusiveness and ownership for process owners (e.g. one-on-one interviews, focus groups)	<ul style="list-style-type: none"> • Use fraud risk workshops to obtain “buy in” from process operators and owners • Invite all relevant employees, regardless of seniority, to attend a workshop
Obtain sufficient knowledge from relevant stakeholders of business processes to facilitate fraud oversight and decision making	<ul style="list-style-type: none"> • Facilitate fraud risk workshops to discuss and map business processes and internal controls • Ask attendees to consider “what could go wrong?” in processes they engage with or manage • Identify areas of fraud risk in a process map that requires internal controls
Engage with relevant stakeholders to obtain feedback and information to support decision-making	<ul style="list-style-type: none"> • Structure emails and/or surveys that focus on fraud risks for specific processes • Adopt appropriate modes of communication

Source: OAG

Table 6: Better practice examples of the communication and consultation stage

⁵ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.2.

One way to enhance communication is by meeting one-on-one to facilitate a better understanding of relevant risk and control issues.

To help with communication and consultation, entities should prepare a communication plan that outlines the intended methods, people and timelines for consultation. This also forms the basis of reporting to any oversight committees on the progress of projects in the fraud risk management program. Examples of methods of communication and consultation are provided in Appendix 5.1.

Scope, context, and criteria

Establishing the scope, context and criteria for the fraud risk assessment is done using the communication and consultation processes outlined above. They will differ for each entity and will be determined by the size and complexity of the process being assessed.



“...Scope, context and criteria involve defining the scope of the process and understanding the external and internal context.”⁶

Case study 1: Example of scope, context and criteria for a risk assessment of selected parts of the Procure to Pay process

Factor	Procure to Pay
Scope	<ul style="list-style-type: none"> • The specific parts of the Procure to Pay process to be assessed are: supplier selection, onboarding vendors, purchase validation (business case, receipt of goods/services) and release of payment. • We will engage with the finance business unit and operational staff responsible for purchase orders and validation of receipt of goods/service. • The entity’s risk assessment policy dated 31 January 2020 will be applied in conjunction with the approved fraud risk assessment program dated 30 June 2021. • As the entity’s procurement staff are across the State, we will need to engage in a number of online meetings with potential site visits. • Timeline: <ul style="list-style-type: none"> ○ engagement with procurement staff by 30 June 2022 ○ identification of risks by 31 October 2022 ○ completion of risk register and mapping of risks by 31 December 2022 ○ first review to Internal Audit and Risk Committee (IARC) by 28 February 2023 ○ second review to IARC by 30 April 2023 ○ submission to Board for approval by 31 May 2023.

⁶ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.3.

<p>Context</p>	<p>Internal factors include:</p> <ul style="list-style-type: none"> the strategic objectives of the entity are: community focused delivery of services, sound business practices and quality services. A list of the specific goods, services or works to be procured are provided in Annexure A the existing employee level in the Procure to Pay process is sufficient, however, their experience is inadequate. No training has been delivered in identifying indicators of potential fraud there is no assessment of fraud controls within vendors the entity has policies and processes in respect of independence for supplier selection panels and purchase validation. <p>External factors include:</p> <ul style="list-style-type: none"> increasing fraud trends targeting procurement and finance teams (i.e. business email compromise - fake emails impersonating an internal senior person or a vendor) recent known scams in the public domain that have been uncovered.
<p>Criteria</p>	<ul style="list-style-type: none"> The below risk criteria are taken from the entity's risk assessment policy dated 31 January 2020. The entity rates likelihood risk on a scale from extremely unlikely to almost certain. Within the Procure to Pay process, rare is conceivable but unlikely, unlikely is conceivable and has occurred in the past but unlikely in the next year. The entity rates consequence risk on a scale from negligible to catastrophic across the following loss factors: financial, reputational, legal, service delivery. Within the Procure to Pay process, negligible has no negative consequence, low disrupts internal non-management process and has no external financial loss, moderate requires corrective action by senior management, potential disciplinary action and minor financial impact etc.

Entities will need to develop a scope, context and criteria for all activities and processes they perform. The CFPC's *Fraud Risk Assessment Leading Practice Guide* provides a strategic profiling tool in support of its recommendation that entities responsible for multiple activities and processes prioritise the areas of the entity that are at higher risk for fraud.

Scope, context and criteria	Better practice
<p>Define the scope of the activity being assessed for fraud risk including objectives and decisions to be made prior to commencing any fraud risk assessment</p>	<ul style="list-style-type: none"> Clearly document the scope and objective of the process that is being assessed for fraud risks Circulate a document that sets out the scope to all employee participating in the fraud risk assessment Break down complex processes into manageable scopes

Scope, context and criteria	Better practice
Establish the context of the fraud risk activity	<ul style="list-style-type: none"> • Understand the external environment • Understand the internal operating environment • Reflect the specific environment of the activity to which the fraud risk management process is to be applied
Align the fraud criteria with an overarching risk management framework used to assess all business risks for consistency	<ul style="list-style-type: none"> • Review the entity's existing risk management framework prior to commencing to ensure up-to-date and fit-for-purpose • Align consequence and likelihood criteria and the risk rating matrix with existing framework
The fraud risk assessment criteria should reflect the organisation's values, objectives and resources and be consistent with policies and statements about risk management	<ul style="list-style-type: none"> • Review the entity's existing risk management policy to understand the entity's risk appetite

Source: OAG

Table 7: Better practice examples of the scope, context and criteria stage

Appendix 5.2 provides a guide on how you could outline your scope, context and criteria.

Risk assessment

Once the scope, context and criteria are established, entities need to assess their fraud risks.

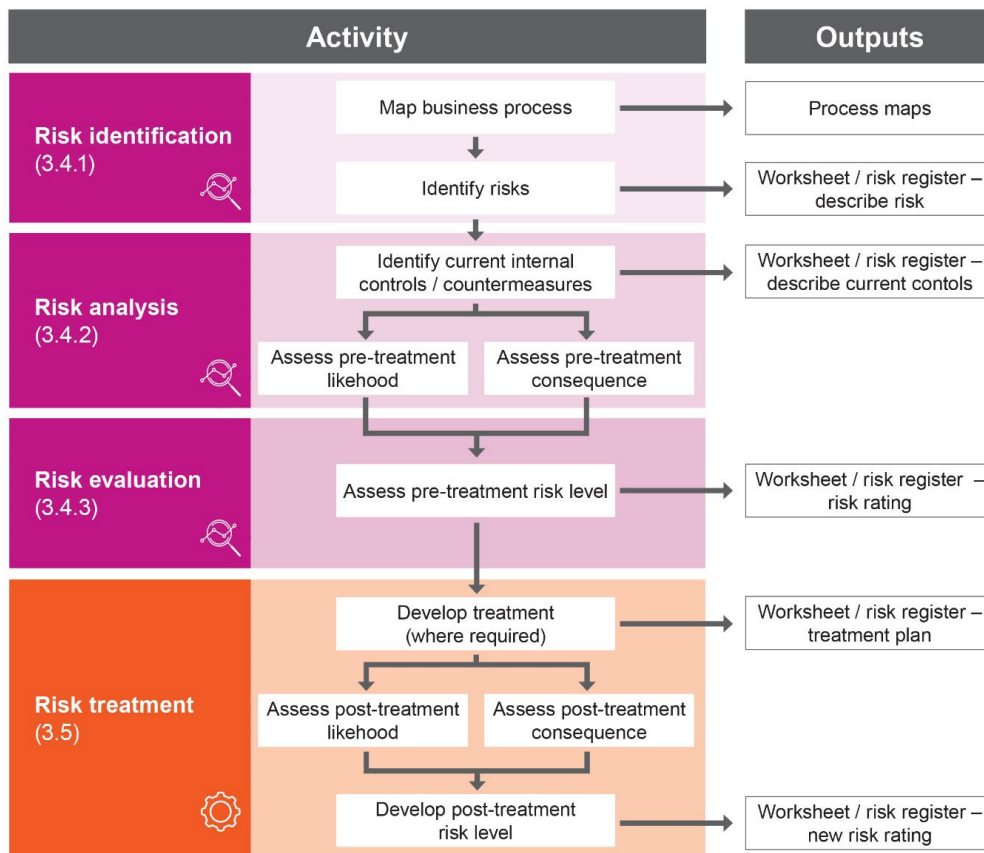
If an entity has a detailed risk assessment approach, then it is logical and likely more efficient to apply that for fraud risks as well.

AS ISO 31000:2018 *Risk Management - Guidelines* sets out 3 sub-phases in the risk assessment stage:

- risk identification
- risk analysis
- risk evaluation.

The assessment stage is followed by treatment. An overview of the risk assessment and treatment stages is set out below.





Source: OAG based on AS ISO 31000:2018 Risk Management - Guidelines Clause 6.4 and 6.5

Figure 5: Risk assessment and treatment stages overview

Identifying risks

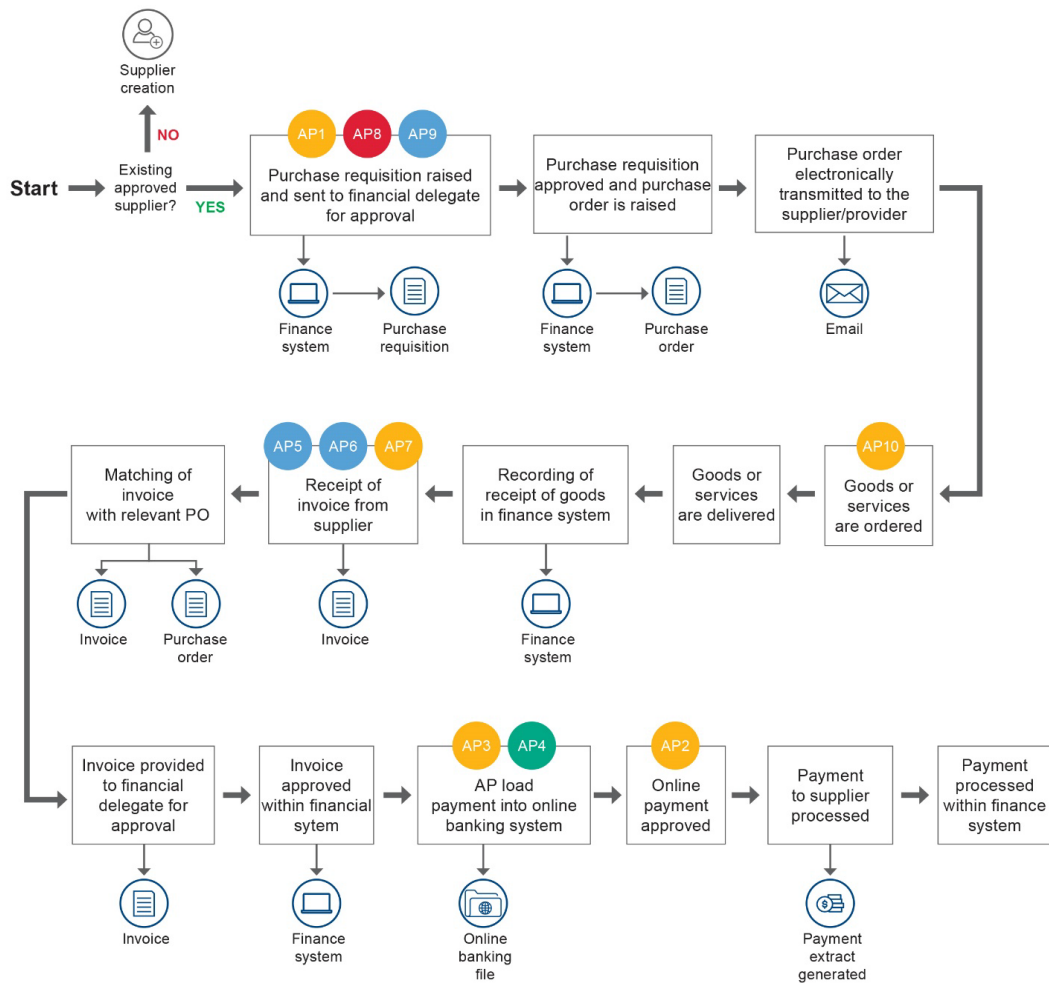
Think like a fraudster. Discover what you don't know.

Risk identification involves:
 "... finding, recognising and describing risks that might help or prevent an organisation achieve its objectives."⁷

It is important to avoid the temptation to be defensive and dismiss risks before they have been properly analysed and evaluated.

Identifying fraud risks should be viewed as a creative process. Brainstorm the various fraud schemes that have and could be committed within or against the entity. An effective way to identify fraud risks is to map the process that is being assessed and identify vulnerabilities within the process. Below is an example of an accounts payable process map, sometimes referred to as a flow chart. The coloured circles represent identified fraud risks in the accounts payable (AP) process.

⁷ AS ISO 31000:2018 Risk management - Guidelines Clause 6.4.2.



Source: OAG

Figure 6: Accounts payable process map

A fraud risk assessment should consider common methods used by fraudsters and look for vulnerabilities within the entity’s processes and activities. This will involve challenging assumptions about, and existing processes within, an entity to identify gaps and thinking of creative ways to circumvent internal controls.

Common frauds are a good place to start but entities should not stop there. Risk identification needs to be realistic but at the same time entities should remember that even the most far-fetched fraud scheme can occur when the right balance of motivation, rationalisation and opportunity are present. Asking hypothetical questions about how fraud could be perpetrated in a structured and controlled way will put the fraud risk assessment process on the right path.

Finally, a good fraud description will allow you to understand ways to prevent or detect the fraud. One way to identify and describe your fraud risks is to consider who did what and what the result was, also described below as the Actor, Action, Outcome method⁸:

⁸ Commonwealth Fraud Prevention Centre, *Fraud Risk Assessment – Leading Practice Guide*.

- actor – accounts payable (AP) officer
- action – submits and processes fictitious invoice
- outcome – payment of invoice results in money going to AP officer's bank account.

Fraud risks that have been identified should be adequately documented on a fraud risk worksheet. Fraud risk worksheets can function as an aid to the risk assessment but also as a fraud risk register and an implementation worksheet.

Appendix 5.3 includes:

- an example of a fraud risk worksheet
- risk assessment and treatment process overview
- key questions you could ask when trying to identify fraud risks
- the CFPC's Actor, Action, Outcome method of describing fraud risks
- an example diagrammatic presentation of assessed fraud risks
- a short summary of fraud risks that are commonly found in the public sector environment. The summary is not intended to be an exhaustive list. The examples in section 2.3 would also be useful in this exercise.

Analysing fraud risks

Once the potential fraud risks within the business unit or process have been identified the next step is to analyse the risks.

Risk analysis is:

*"... a detailed consideration of uncertainties, resources, consequences, likelihood, events, scenarios, controls and their effectiveness."*⁹

Fraud risk analysis requires input from employees within the business unit(s) being assessed and any additional subject matter experts who can add value to the process.

An analysis of each risk includes considering:

- **the likelihood** of the risk occurring
- **the consequence** for the entity if it did occur
- **resourcing constraints** impacting controls
- **the effectiveness of existing controls** intended to mitigate the risks.

The entity should use its established risk analysis matrix to analyse the likelihood, consequences, and strength of existing controls to assign a risk rating to each fraud risk. It is critical that every business unit within an entity use the same risk analysis matrix to allow for a proper comparison of risks across the entity.

Figure 7 below is an example of a risk assessment matrix that shows the likelihood combined with the consequences risks results:

⁹ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4.3.

Likelihood		Consequence				
		Negligible	Low	Moderate	Major	Extreme
	Almost Certain	Medium	High	Very High	Very High	Very High
	Likely	Medium	High	High	Very High	Very High
	Possible	Low	Medium	High	High	Very High
	Unlikely	Low	Low	Medium	High	High
	Rare	Low	Low	Low	Medium	Medium

Source: OAG

Figure 7: Example of a risk assessment matrix

Sometimes an entity undertaking a fraud risk assessment can overestimate the effectiveness of internal controls. One technique to fully assess their effectiveness is to conduct a walk-through of the relevant process or activity and determine if the controls are currently operating effectively. Applying a sceptical approach to the controls and adopting the mindset of a determined fraudster can help to assess if a control can be overridden or avoided. Internal audit resources can also be helpful in this assessment.

Risk analysis	Better practice
Consider uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness	<ul style="list-style-type: none"> Detailed documentation of the analysis including reasoning for decisions for example if a risk is determined to be HIGH for consequence document why and what inputs were used
Events can have multiple causes and consequences and affect multiple objectives	<ul style="list-style-type: none"> Deep dive analysis to identify all causes, both internally, externally and potential consequences
Scrutiny of existing controls	<ul style="list-style-type: none"> Sufficiently analyse and test existing controls including walk-throughs and penetration testing Consider engaging specialists to identify gaps in existing system controls

Source: OAG

Table 8: Better practice examples of the risk analysis stage

Evaluating fraud risks

Once an entity’s fraud risks have been analysed, they need to be evaluated against the entity’s risk appetite and tolerance. This should be defined in the entity’s risk management policy and framework. The evaluation is used to determine if further action is required to reduce identified residual risks to an acceptable level.

Entities’ risk appetites and tolerances vary and depend on factors such as the circumstances of a particular program, the cost-benefit of implementing controls to reduce the risk of fraud, resources or other constraints and reputational risk. Risk tolerance is not static and should be determined on a case-by-case basis for each risk identified.

The purpose of risk evaluation is to:

“... support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.”¹⁰

It is important that the evaluation of fraud risks involves detailed input from the process and risk owners and includes senior employees who can consider the cost of countering fraud against the entity’s risk tolerance. The evaluation considers the residual fraud risk and should conclude with one of the following outcomes¹¹:

- avoid the risk
- accept the risk
- remove the risk source
- change the likelihood
- change the consequences
- share the risk
- retain the risk.

These conclusions, and links to any supporting documentation, should be included in the fraud risk assessment worksheet.

Risk evaluation	Better practice
Evaluate results from risk assessment	<ul style="list-style-type: none"> • Comparing the results of the risk analysis with the established risk criteria to determine if and where additional action is required
Record and communicate evaluation results	<ul style="list-style-type: none"> • Risk evaluation outcomes are recorded, communicated and then validated at appropriate levels of the organisation

Source: OAG

Table 9: Better practice examples of the risk evaluation stage

Risk treatment

After finalising the risk assessment, the risk treatment process is undertaken. An entity’s evaluation of the risks and its risk appetite will determine if the residual risk is at an acceptable level or if treatment is required. Risk treatments can include enhancing existing controls, implementing new controls, or avoiding the risk altogether by no longer undertaking the activity, program or service.



An entity needs to consider how to mitigate the residual fraud risks that remain above the entity’s tolerance level. The objective of treating the fraud risk is to reduce the residual risk identified in the assessment to an acceptable level.

¹⁰ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4.4.

¹¹ AS ISO 31000:2018 *Risk management - Guidelines* Section 6.5.2.

The aim of risk treatment is to:
 “.. *select and implement options for addressing risk.*”¹²

An overview of the risk treatment process has been set out in Figure 5.

Some treatments may enhance existing controls or introduce new controls. Fraud controls are specific measures, processes or functions that are intended to prevent or detect fraud events or to enable the entity to respond to them. These would be suitable to address the following outcomes:

- accept the risk
- change the consequence
- change the likelihood
- change both the consequence and likelihood
- share the risk
- retain the risk.

Subject to the entity’s risk appetite and tolerance, not every risk will require the development and implementation of treatments.

Risk treatment	Better practice
Determine appropriate risk treatments	<ul style="list-style-type: none"> • Select risk treatment options with the entity’s objectives, risk criteria and available resources • Balance the potential benefits against cost, effort or disadvantage of implementation
Document implementation plan	<ul style="list-style-type: none"> • Document the treatment plan outlining the responsibilities, resources and other relevant implementation information in the fraud risk worksheet
Risks that do not have a treatment option	<ul style="list-style-type: none"> • If no treatment options are available or if treatment options do not sufficiently modify the fraud risk, the risk is recorded and kept under ongoing review
Remaining risk is documented	<ul style="list-style-type: none"> • Inform decision makers and other stakeholders of the nature and extent of the remaining risk after treatment • Document the remaining risk and subject to monitoring, review and, where appropriate, further treatment
Consider beyond economic consequences	<ul style="list-style-type: none"> • Justification for risk treatment is broader than solely economic consequences and considers the entity’s obligations, voluntary commitments and stakeholder views

Source: OAG

Table 10: Better practice examples of the risk treatment stage

¹² AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.5.

A useful way to examine your controls is to ensure they are specific, measurable, achievable, relevant and timed (SMART). This model and examples of internal controls that may be applied with a view to change the consequence, likelihood or both are provided at Appendix 5.4.

Monitoring and review

Entities should actively monitor the implementation of fraud risk treatments, because until the new or improved controls are in place, the fraud risk will remain above this tolerance level. Fraud risk owners will be responsible for ensuring the controls are implemented in a timely manner and remain effective. When a new or improved control has been implemented the entity should review the control in practice over time to ensure it continues to be effective.



Further, it is essential that entities have a program to continuously monitor and review their fraud risks. Sometimes only small changes to a business process or function can alter the inherent fraud risk rating, result in the emergence of new fraud risks, or impact the effectiveness of existing controls.

Monitoring and review is:
“... to assure and improve the quality and effectiveness of process design implementation and outcomes.”¹³

Monitoring and review	Better practice
Monitoring and review takes place during all elements of fraud risk management program	<ul style="list-style-type: none"> Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback
Monitoring and review progress is reported	<ul style="list-style-type: none"> Results of monitoring and review are incorporated throughout the entity’s performance management, measurement, and reporting activities

Source: OAG

Table 11: Better practice examples of the monitoring and review stage

Recording and reporting

As noted earlier, fraud risks identified through a fraud risk assessment can be integrated into the entity's broader enterprise risk register. Whether entities combine all risks into a single source risk register or maintain a separate fraud risk register, they must be documented and reported. Entities should report to appropriate oversight committees and management including any audit committees which are responsible for overseeing the entity risk management and internal controls.



Risk management process and its outcomes should be:
“... documented and reported through appropriate mechanisms.”¹⁴

¹³ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.6.

¹⁴ AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.7.

The fraud risk assessment worksheet details several key processes and outcomes that should be documented including the methodology for the risk assessment, the results and the response.

Recording and reporting	Better practice
Detailed recording of fraud risk assessment process	<ul style="list-style-type: none"> Worksheets include adequate information that demonstrates reason for decisions made and actions taken
Ongoing monitoring and periodic review of the fraud risk management process and its outcomes is planned, and responsibilities clearly defined	<ul style="list-style-type: none"> Updates provided to senior management and those charged with governance on progress Monitoring through audit committee Documented responsibilities for undertaking fraud risk management are outlined in the entities' FCS

Source: OAG

Table 12: Better practice examples of the recording and reporting stage

Conclusion

Fraud is a pervasive and growing issue within Australia. Fraud can be initiated by employees or close associates of an entity and, increasingly, by parties with no apparent connection to the entity. It can also involve collusion between internal and external parties.

Historically, the approach of many Australian entities to fraud risk management has been wholly reactive. Entities that embrace adequate and proportionate approaches to managing fraud risks will increase their chance of reducing fraud events.

We encourage entities to use this guide along with the tools and any other available resources when applying AS ISO 31000:2018 – *Risk management - Guidelines* and AS 8001:2021 – *Fraud and corruption control* to manage the risk of fraud against their entity. While fraud risks cannot be eliminated, a robust and well-resourced fraud risk management program can minimise the likelihood and consequences of fraud events.

Appendix 1: Glossary

Term	Definition
Better practice guide (BPG)	A fraud risk assessment better practice guide (this report).
Bribery	Offering, promising, giving, accepting or soliciting of an undue advantage of any value (either financial or non-financial) directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties.
Cloud computing	The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
Close associate	A person with a close connection with the organisation other than an employee (e.g. director, consultant, contractor).
Collusive tendering	The act of multiple tenderers for a particular contract colluding in preparation of their bids – also often referred to as bid rigging.
Conflict of interest	A situation in which a person is in a position to derive personal benefit from actions or decisions made in their official capacity.
Corruption	Dishonest activity in which a person associated with an entity (e.g. director, executive or employee) acts contrary to the interests of the entity and abuses their position of trust in order to achieve personal advantage or advantage for another person or entity.
Cryptocurrency	A digital currency in which transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralised authority.
Data theft	Also known as information theft. The illegal transfer or storage of personal, confidential, or financial information.
Enterprise risk	Risks arising from the general operation of an entity that can impact on the entity's ability to meet its objectives (refer also definition of 'risk' below).
FCS	Fraud Control System - a framework for controlling the risk of fraud against or by an entity.
Fraud	Dishonest activity causing actual or potential gain or loss to any person or entity including theft of moneys or other property by persons internal and/or external to the entity and/or where deception is used at the time, immediately before or immediately following the activity.
Identity fraud	Also known as identity theft or crime. It involves someone using another individual's personal information without consent, often to obtain a benefit.
Internal control	Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance that information is reliable, accurate and timely.
Malware	Malicious software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorised access to information or systems, deprive user's access to information or which unknowingly interferes with the user's computer security and privacy.

Term	Definition
Nepotism and/or Cronyism	Where the appointee is inadequately qualified to perform the role to which he or she has been appointed. The appointment of friends and associates to positions of authority, without proper regard to their qualifications.
OAG	The Office of the Auditor General.
PESTLE model	Consideration of 6 external environmental factors that can impact an entity, namely the political, economic, social, technological, legal and environmental factors.
Phishing and/or Spear-phishing	Cyber-intrusion. Theft of intellectual property or other confidential information through unauthorised systems access.
Ransomware	Form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
Risk appetite	The level of overall risk an entity is prepared to accept in pursuing its objectives.
Risk tolerance	The level of risk an entity is prepared to accept in relation to specific aspects of its operation – the practical application of the concept of 'risk appetite' to specific risk categories (relevantly to the subject of this guide, this can include application of an entity's risk appetite to the concept of fraud risk).
Social engineering	A broad range of malicious activities accomplished through human interactions (e.g. psychological manipulation of people into performing actions or divulging confidential information).

Appendix 2: References

Reference
Association of Certified Fraud Examiners , 2022.
Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations , 2022.
Australian Cyber Security Centre Australian Cyber Security Centre analysis , 2022.
Commonwealth Fraud Prevention Centre, Fraud Risk Assessment Leading Practice Guide , 2022.
Cressy, D., <i>Other People's Money: A Study in the Social Psychology of Embezzlement</i> , Free Press, 1953.
Department of Justice, Corporations Act 2001 , 2001.
Department of Justice, Western Australia Corruption, Crime and Misconduct Act 2003 , 2022.
Department of Justice, Western Australia Financial Management Act 2006 , 2022.
Department of Justice, Western Australia Government Financial Responsibility Act 2000 , 2021.
Department of Justice, Western Australia Procurement Act 2020 , 2021.
Department of Justice, Western Australia Public Interest Disclosure Act 2003 , 2017.
Department of Justice, Western Australia Public Sector Management Act 1994 , 2022.
Department of Treasury, Treasurer's Instructions – specifically TI 825 Risk Management and TI 304 Authorisation of Payments , 2022.
Enacting legislation for GTEs and other government bodies
Office of the Auditor General Western Australia, Forensic Audit Report – Establishment Phase , November 2021.
Office of the Auditor General Western Australia, Fraud Prevention and Detection in the Public Sector , June 2013.
Public Sector Commission WA, Integrity Strategy for WA Public Authorities , 2019.
Standards Australia, AS 8001:2021 – Fraud and corruption control , June 2021.
Standards Australia, AS ISO 37001:2019 Anti-bribery management system , 2019.
Standards Australia, AS ISO 31000:2018 Risk management – Guidelines Risk Assessment , 2018.
Standards Australia, SA SNZ HB 436-2013 Risk Management Guidelines (companion to AS ISO 31000:2018) , 2013.

Appendix 3: Fraud control system benchmarking tool

An important component of the periodic assessment of the efficacy of an entity's FCS is to determine whether an entity's FCS aligns with the requirements and guidance set out in the standard, in effect, a benchmarking of the entity's fraud control program against the requirements and guidance of the standard. An organisation's performance against each element of the standard can be assessed in accordance with a 5-element rating scheme as set out below.

Alignment with AS 8001:2021 – Fraud and corruption control best practice model		Rating
Meeting better practice		5
Approaching better practice		4
Minimum acceptable level		3
Inadequate but some progress made towards better practice		2
Inadequate - no progress towards achieving better practice		1

The following are the relevant steps required to prepare and deliver an FCS benchmarking project:

Step 1	Consult and collaborate across the entity in a consideration of the FCS benchmarking model and determine which, if any, elements of the model are not relevant to the entity's own circumstances, make necessary adjustments to the model in preparation for analysis. ¹⁵
Step 2	Gather all entity documentation pertaining to the control of fraud risk within the entity – this would include: <ul style="list-style-type: none"> • current FCS documentation • current governing body charter • most recent fraud risk assessment • the entity's disciplinary procedures • recent analysis of awareness raising activities within the entity • most recent external environmental scan analysis

¹⁵ e.g. requirements and guidance of AS 8001:2021 Section 3.6 Performance Based Targets may not be relevant to public sector entities and could therefore be removed from the model.

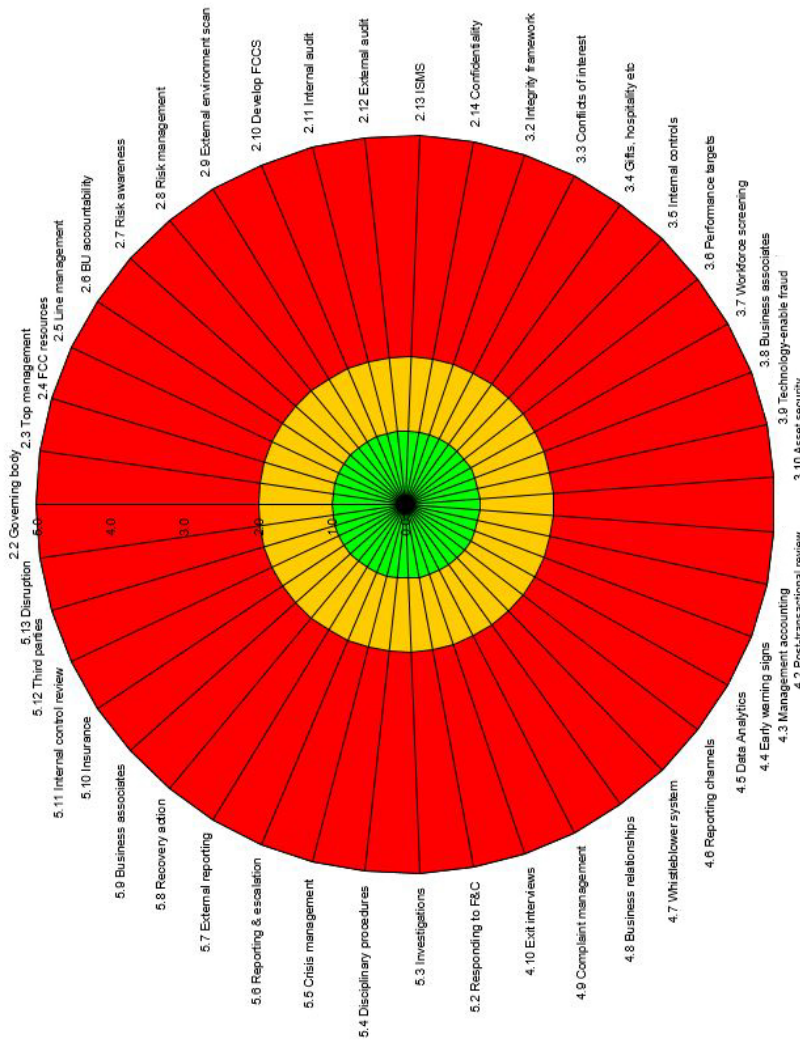
	<ul style="list-style-type: none"> internal audit charter any recent internal audit reports in relation to fraud risk management all integrity related documentation current workforce screening policy current cybersecurity / information system management policies a summary of the last 5 years fraud incidents covering results could provide insight into common activities, themes and weaknesses. Details such as number of events per year, fraud theme (procurement, CC etc), quantum, fraud substantiated Y/N, vulnerability identified, how vulnerability treated, date vulnerability treated reports of analysis of internal control efficacy including pressure testing transactions.
Step 3	<p>Consult broadly across the entity to arrive at a realistic and reliable assessment of the entity's current performance against each relevant element of AS8001:2021. Consultation would include:</p> <ul style="list-style-type: none"> if a relevant policy or procedure is currently in place or is proposed the frequency of review of all relevant policies and procedures if there is adequate resourcing to ensure that the FCS is properly and effectively administered the culture within the entity in terms of adherence to the key elements of the FCS.
Step 4	<p>Collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its current alignment with AS 8001:2021.</p>
Step 5	<p>Consult broadly within the organisation in relation to initiatives currently in train for implementation in the future, collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its future alignment with AS 8001:2021 on the assumption that the initiative is fully implemented.</p>
Step 6	<p>Enter scores into the model and review the output chart.</p>
Step 7	<p>Present to the relevant oversight committee within the entity.</p>
Step 8	<p>Implement remedial action required for the entity to better align with the better practice model per AS 8001:2021.</p>
Step 9	<p>Monitor the ongoing efficacy of the FCS in light of this analysis over time.</p>

Presentation of the benchmarking analysis

The outcome of this analysis can be usefully presented in a variety of tabular or graphical formats. The way in which the benchmarking analysis results are presented will depend on the needs of the entity. One particularly visual way of presenting the outcomes of the benchmarking analysis is by way of a 'spider-web' diagram as shown below.

A Microsoft Excel tool is provided on our website with detailed instructions to assist in the preparation of this analysis and production of the spider web diagram is detailed below.

The spider web diagram is particularly useful for presenting current and future state alignment of an entity's FCS with AS 8001:2021 and for showing improvement over time. For example, if a spider web diagram depicting the current and anticipated alignment of the entity's FCS with AS 8001:2021 is presented to each meeting of the relevant oversighting committee (e.g. an audit committee) the committee would be able to efficiently monitor progress against action items initiated to address identified gaps.



The green area	Represents the entity's current alignment with the requirements and guidance of AS 8001:2021.
The amber area	Represents the entity's anticipated future alignment with the requirements and guidance of AS 8001:2021 once initiatives currently in train are fully implemented. Theoretically, the amber area should progressively turn to green over the projected implementation timeframe.
The red area	Represents the current 'gap' between either the current alignment (green) or anticipated future alignment (amber) with the requirements and guidance of AS 8001:2021.

Appendix 4: External threat assessment tool

Assessment of external threats using the PESTLE model requires a rigorous 7-step process as follows:

- Step 1:** Consult and collaborate across the entity, make necessary adjustments to the worksheet in preparation for analysis.
- Step 2:** Gather all documentation pertaining to external threats in the environment in which the entity operates or is considering operations.
- Step 3:** Consider the most recent fraud risk assessment conducted in relation to the entity's operation.
- Step 4:** In collaboration with risk and process owners, consider the six PESTLE factors that could impact the entity's fraud risks.
- Step 5:** Identify external factors that need to be addressed by the entity to more effectively control fraud risks.
- Step 6:** Develop risk treatments for risks that need to be further mitigated and adjust in fraud risk assessment and fraud control system.
- Step 7:** Review external threats periodically.

The following is an example worksheet for assessing external threats against an entity using the PESTLE model.

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
Political			
To identify the political situation of the country in which the organisation operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and international political pressure.	<ol style="list-style-type: none"> Has there been a recent change in government (at local, state or federal level)? Is there any anticipated change in government funding foreshadowed? How will a change in funding impact the entity's fraud exposure (e.g. an increase in funding for grants or a decrease in funding for administration)? Is there any legislative change anticipated in relation to employment law that may impact the entity's ability to manage its fraud exposure? 	Insert text	Insert text

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	<ol style="list-style-type: none"> 4. Is there a likely increase or reduction in government mandated regulation? 5. If yes, will that give rise to an increase in the entity's fraud exposure (either internally or externally initiated fraud)? 6. Are there any other political factors the entity should consider? 		
Economic			
<p>To determine the economic factors that could have an impact on the organisation, including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.</p>	<ol style="list-style-type: none"> 1. Are all economies in which the entity operates currently stable? 2. If there are indications of instability in an economy in which the entity operates, to what degree will this impact the risk of fraud within or against the entity? 3. Are there any key economic decisions (either recently implemented or in contemplation) likely to have an impact on the entity's fraud exposure (e.g. rising interest rates, a change in taxation rates)? 4. Is there currently significant pressure on wages and salaries that could act to reduce disposable income of the general population and to what degree could that impact on the entity's fraud exposure? 5. Is there likely to be a change in employment levels in the economy in the next three to five years? 	<p>Insert text</p>	<p>Insert text</p>

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	6. Is there likely to be a change in working arrangements that may increase the risk of fraud within the entity (e.g. remote working, flexible working arrangements)? 7. Are there any other economic factors the entity should consider?		
	Social To identify the expectations of society by analysing factors such as consumer demographics, significant world events, integrity issues, cultural, ethnic and religious factors, and consumer opinions.	Insert text	Insert text
	1. Has there been a marked decline in integrity standards within the broader community or is this anticipated going forward? How could these changes impact the entity's fraud exposures in the future? 2. Is it likely that the entity will only be able to attract adequate human resource is by offering work arrangements that are not sustainable for the entity? 3. Are there any other social factors they should consider?	Insert text	Insert text
	Technological To identify how technology, including technological advancements, social media platforms and the role of the internet more broadly, is affecting or could affect the organisation.	Insert text	Insert text

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	and the general public? 3. Does the entity embrace leading edge cyber-security? 4. Does the entity have strict policies governing the use of its IT equipment by the workforce for personal purposes? 5. Does the entity have strong controls over the use of technology in the course of remote working? 6. Does the entity closely monitor developments in technology-enabled fraud? 7. Are there any other technological factors that the entity should consider?		
	Legal To identify how specific legislation, including industry specific regulations, and case law are affecting or could affect the organisation's future operations.	1. Does the entity have a strong compliance function? 2. Does the entity have a strong sense of its own duties of integrity when interacting with external parties (i.e. is there a risk of the entity itself being accused of fraudulent or other illegal conduct)? 3. Are there indicators of significant change in the regulatory landscape affecting the entity? 4. Is the entity aware of its vicarious liabilities in relation to the conduct of members of its own	

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	workforce? 5. Are there any other legal factors that the entity should consider?		
Environmental			
To identify how local, national and international environmental issues are affecting or could affect the organisation.	<ol style="list-style-type: none"> 1. Does the entity operate in circumstances where there is a likelihood of a high environmental impact? 2. If so, does this give rise to any raised risk of manipulation of financial or non-financial reporting? 3. Are there any other environmental factors that the entity should consider? 		

Appendix 5: Tools to support the fraud risk management process



A5.1 Communication and consultation tool

Fraud risk owners can sometimes encounter problems with those responsible for developing, implementing and maintaining fraud controls relating to their risks. This may be because a control owner is experiencing staffing or funding constraints or they lack the requisite expertise. In these circumstances the person tasked with performing the fraud risk program can assist through:

- requesting progressive pieces of work
- fostering productive linkages between parties responsible for fraud control
- providing expert advice to stakeholders
- seeking strategic support from the senior staff to formulate solutions to impediments at the operational or program level.

The table below describes some methods for communication and consultation across an entity.

<p>Structured one-on-one discussion with the process / risk owners</p>	<p>Speak with relevant business units – the people who work with the systems and processes every day. Meet one-on-one to facilitate an enhanced understanding of relevant risk and control issues.</p>
<p>Convene focus groups with process and risk owners and stakeholders</p>	<p>Facilitate detailed discussion of fraud risks with focus groups along with one-on-one meetings as an effective way to identify risks, internal controls that should mitigate those risks, whether they are operating as intended (think like a fraudster), assessing risks and developing effective risk treatments.</p>
<p>Seek input on fraud risk matters from across the entity</p>	<p>Invite the entire workforce to provide their input in relation to the entity's fraud exposures in an online survey.</p>
<p>Regular reporting to the project management committee</p>	<p>A project to manage fraud risk should be subject to a rigorous program of two-way communication between the oversight committee and the practitioner/team tasked with the project.</p>
<p>External communication and consultation</p>	<p>The project committee and the team responsible for delivering the project should consider the benefits of communication and consultation with parties external to the entity such as regulators, subject matter experts and peer organisations.</p>
<p>Reporting to the audit and risk committee</p>	<p>It is important for an audit and risk committee to be informed of developments in relation to fraud risks because they are responsible for overseeing the entity's risk management and internal controls.</p>



A5.2 Scope context and criteria tool

Fraud risk assessment “XX Process”	
Factor	Definition
Scope	<p>The boundaries within which the fraud risk assessment will take place.</p> <ul style="list-style-type: none"> The specific parts of the XX process to be assessed for fraud risks. The business units and operational teams involved in the processes to be assessed. Tools to be used in the fraud risk assessment. Logistical considerations, milestones and timelines for completing the fraud risk assessment.
Context	<p>The internal and external factors influencing the environment the entity operates in.</p> <p>Internal factors may include:</p> <ul style="list-style-type: none"> The strategic objectives of the entity and how this influences the XX process. The existing employee level in the XX process and their experience, as well as their level of training in identifying indicators of potential fraud. <p>External factors include:</p> <ul style="list-style-type: none"> Increasing fraud trends targeting XX process. Recent known scams in the public domain that have been uncovered.
Criteria	<p>Likelihood and consequence criteria aligned to an entity’s existing risk framework that can be used to rate fraud risks identified in the fraud risk assessment.</p> <ul style="list-style-type: none"> Likelihood criteria is a rating scale (i.e Extremely unlikely to Almost certain) set by the entity to identify the expected frequency of a fraud risk in the XX process being realised, both with no internal controls in place (inherent) and existing controls in place (residual). Consequence criteria is a rating scale (Low – Catastrophic) across a number of defined loss factors (i.e. financial damage, reputational damage, legal damage), to identify the expected impact of a fraud risk in the XX process being realised both with no internal controls in place (inherent) and existing controls in place (residual). What is acceptable frequency / consequence.



A5.3 Risk assessment tools

A5.3.1 Example fraud risk assessment worksheet

A fraud risk assessment worksheet can be used to document all relevant information for each risk identified and assessed. Having applied the worksheet for this purpose it can also then be used as a risk register (alternatively, identified and assessed fraud risks could be included in the entity's enterprise risk register).

Fraud Risk (Short Title)		Risk Level		Description of Risk		
AP 1	Corruption in procurement (kickbacks)	Pre-treatment Very High	Post-treatment High	Procurement employee obtains a benefit from a supplier on the understanding that the employee will award work to the supplier.		
Current Internal Controls		Overall Ratings		Proposed Treatment (if Applicable)		
Rating		System Business Unit		Rating Responsibility		
Documented policies and procedures for procurement transactions >\$50,000 are in place.	Partially Effective	Pre-treatment	Internal Control	Training and awareness initiatives for staff.	Effective HJG	High
Conflict of interest declaration forms are required to be completed by all staff.	Effective	Consequence	Likelihood	Regular review of the conflict of interest declaration register.	Effective HJG	Medium
Independent evaluation of tender bids are undertaken	Ineffective	Post-treatment	Likelihood	Documented evaluation reports to be prepared and submitted to those charged with governance.	Effective HJG	High
Missing control: There is no regular transaction review of purchases over \$50,000.	Ineffective	Internal Control	Consequence	Finance to review regular reports (i.e. monthly) with expenditure broken down by vendor.	Effective HJG	Medium
Due diligence is performed on successful vendors.	Partially Effective	Likelihood	Likelihood	Due diligence checks should include open source information background checks on Directors.	Effective HJG	Low
An independent party reviews any vendor complaints from the tender process.	Partially Effective	Internal Control	Likelihood			
Risk Owner HJG	Department Procurement	System Business Unit Accounts Payable	Entered By JNH	Division Finance	Date Assessed 13 May 22	

The following is a short summary of the information that would be recorded on each risk assessment sheet (note that much of the information referred to in the following table will not have been prepared in the risk identification stage when the fraud risk worksheet is first created. The worksheet is intended to build over time as the entity works its way through the identification, analysis, evaluation and treatment development phases).

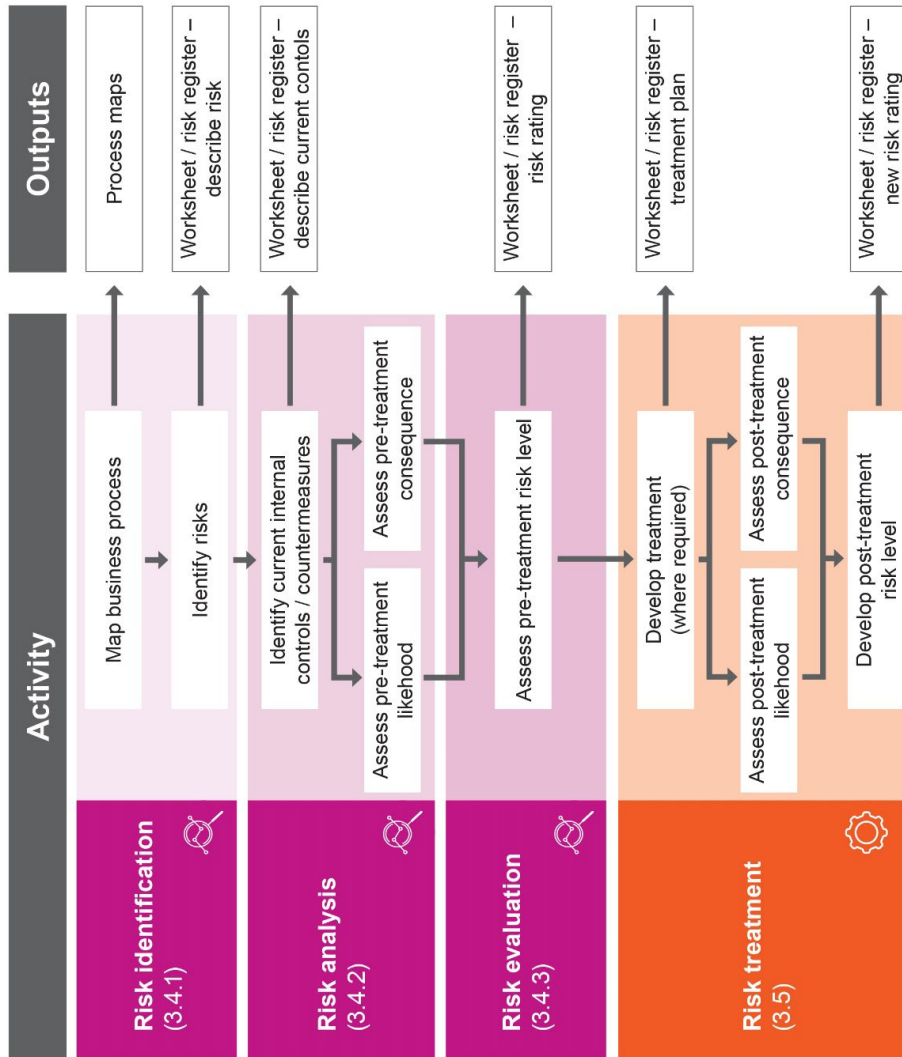
As noted above, each identified risk should be recorded on a separate risk assessment worksheet. The risk assessment worksheet can then be used as the entity's register of fraud risks. Alternatively, identified and assessed fraud risks can be recorded in the entity's enterprise risk register.

Data field	Information to be recorded (for each risk)
Fraud Risk Number	A reference number unique to each risk – the risk number is used in all outputs of the risk assessment process.
Fraud Risk (Short Title)	Short description of the risk that is generally used to identify the risk being discussed in relevant outputs.
Description of Risk	A more detailed outline of the risk consistent with the short title.
Risk Owner	The individual or position within the business unit who has primary responsibility for the business systems relevant to the identified fraud risk.
Department	The department to which the business unit belongs (see below).
System Business Unit	The business unit that has most control of the business systems and processes relevant to the identified risk.
Entered By	The individual or position who entered the fraud risk particulars into the risk assessment worksheet.
Date Assessed	The date on which the worksheet was populated.
Current Internal Controls	A short active title / description of each existing internal control (e.g. "System controls only allow limited authorised users to change bank accounts") and a short statement as to how the internal control mitigates the risk.
Current Internal Controls Rating	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the effectiveness of each internal control on mitigating the risk.
Proposed Treatment (If Applicable)	Treatments the entity proposes to take to strengthen the existing internal control framework and reduce the risk rating to an acceptable level.
Proposed Treatment (If Applicable) Rating	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the effectiveness of each treatment on mitigating the risk.
Proposed Treatment Priority	The proposed priority of the treatment.
Overall Ratings – Pre-treatment Internal Control	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the overall effectiveness of the existing internal control framework on mitigating the risk.

Data field	Information to be recorded (for each risk)
Overall Ratings – Pre-treatment Likelihood	A rating on an appropriate scale (i.e. “Almost Certain” to “Rare”) of the likelihood of a risk being realised with the existing internal control framework.
Overall Ratings – Pre-treatment Consequence	A rating on an appropriate scale (i.e. “Extreme” to “Negligible”) of the consequence of a risk being realised with the existing internal control framework.
Overall Ratings – Post-treatment Internal Control	A rating on an appropriate scale (i.e. “Ineffective”, “Partially Effective” or “Effective”) of the overall effectiveness of the post-treatment internal control framework on mitigating the risk.
Overall Ratings – Post-treatment Likelihood	A rating on an appropriate scale (i.e. “Almost Certain” to “Rare”) of the likelihood of a risk being realised with the post-treatment internal control framework.
Overall Ratings – Post-treatment Consequence	A rating on an appropriate scale (i.e. “Extreme” to “Negligible”) of the consequence of a risk being realised with the post-treatment internal control framework.
Overall Risk Rating Pre-treatment	A rating on an appropriate scale (i.e. “Very High” to “Low”) of the fraud risk level by reference to the risk matrix (taking into account the assessed effectiveness of pre-existing internal controls).
Overall Risk Rating Post-treatment	A rating on an appropriate scale (i.e. “Very High” to “Low”) of the fraud risk level by reference to the risk matrix taking into account the assessed effectiveness of the post-treatment internal control framework.



A5.3.2 Risk assessment and treatment process overview



Source: OAG based on AS ISO 31000:2018 Risk management - Guidelines Clause 6.4 and 6.5



A5.3.3 Key fraud risk identification questions

Some key questions to ask when trying to identify fraud risks are listed below.

Key questions that need to be asked in identifying fraud risks
If I wanted to steal from this entity, knowing what I know about the current business systems process and internal controls, how would I do it?
If I wanted to get some sort of improper financial or non-financial advantage out of my position, how would I do it?
What do I know about this process that nobody else knows or checks?
Who has sole control over specific systems or processes that nobody else has visibility over?
What forms of payment does this process have – is it cash, card, EFT etc?
How can this process be made easier for the process owner at the expense of the entity?

A5.3.4 Commonwealth Fraud Prevention Centre's 'Actor, Action, Outcome' method of describing fraud risks¹⁶

An effective method for describing fraud risk is to consider the actor, action and outcome. The level of detail is important when describing fraud risks. Without sufficient detail it becomes difficult to consider the factors (i.e. actors and actions) that contribute to the fraud risk and how fraud controls will specifically address these contributing factors.

An example of a poorly defined fraud risk from the invoice payment process provided would be "Fraud in the invoice payment process".

The following are more accurately defined fraud risks from the same example:

- "a service provider (Actor) submits a falsified invoice (Action) to receive a payment for services not provided (Outcome)"
- "a service provider (Actor) coerces an official to approve and/or process a falsified invoice (Action) to receive a payment for services not provided (Outcome)"
- "an official (Actor) manipulates the finance system (Action) to divert an invoice payment to their own bank account (Outcome)".

Judgement should be applied in striking a balance between capturing sufficient detail and documenting a manageable number of fraud risks. This could be achieved by combining similar risks and clearly documenting the various contributing factors (actors and actions).

¹⁶ Commonwealth Fraud Prevention Centre 'Fraud Risk Assessment – Leading Practice Guide'.

The description can help with an entity's assessment of its fraud risks and how it considers ways in which to control it. Some of these controls may already exist and some may be new.

For example, an entity might limit the opportunity for an accounts payable officer to submit and processes a fictitious invoice that pays into an employee's account by:

- splitting the authorising powers (submit and process)
 - segregation of duties between invoice entry and payment authority
- validating the invoice details (fictitious invoice)
 - third party verification of goods/services being received
- check supplier details in your supplier master file are an exact match to public records (e.g. Australian Business Register)
- cross-checking internal records (employee account)
 - compare bank accounts in supplier payment file against employee bank accounts.

Entities can link each of the above controls back to distinct parts (actor, action, outcome) of the fraud description.



A5.3.5 Example diagrammatic presentation of assessed fraud risks

It can be useful to present identified and assist fraud risks in diagrammatic form.

The following example shows the relative ratings of likelihood and consequence and the resulting overall risk rating for ten accounts payable related fraud risks. Diagrammatic analysis is also useful to show the projected change in risk rating as a result of implementation of a treatment plan introducing new or revised internal controls / fraud controls. The change in rating in relation to risk PR-1 is due to the introduction of new or revised internal controls that will reduce the consequence of the risk if it did occur (although in this example the likelihood remains unchanged).

Accounts payable





A5.3.6 Example public sector fraud risks

The following is a short summary of fraud risks that are commonly found in the public sector environment. This summary is not intended to be an exhaustive list, but it can be used as a ‘thought provoker’ in the identification of operational risks types facing the entity being assessed.

Accounts payable fraud	
False invoicing (creation of a fictitious vendor)	A fictitious vendor is created in the finance system to which payments for false invoices are made for goods/services not ordered and not delivered (typically fraud of this type involves personnel within the entity but it can be perpetrated at times by external parties acting alone or by external parties operating in collusion with a member of the target entity’s workforce)
Fraudulent change to vendor master file	Fraudulent change to the entity’s vendor master file (i.e. change of bank details to divert legitimate vendor payments to an account controlled by the perpetrator) – this can be done by a person internal to the entity, a person external to the entity or by collusion between internal and external persons
Online banking fraud	Manipulation of vendor or other payments in the online banking system immediately prior to execution of the payment file in the entity’s online banking system – the fraudulent manipulation of the online payment file is concealed by making false entries in the entity’s accounting records
False invoicing (existing vendor)	Manipulation and processing of fraudulent payments for invoices apparently rendered by a legitimate vendor but, in fact, fraudulently generated and issued by the perpetrator who is generally a member of the entity’s own workforce
Duplicate payments for the invoices already settled	More than one payment is made for the same invoice – this can be initiated inadvertently by a vendor who issues the same invoice twice in error but the vendor then fails to report the double receipt and fraudulently converts the duplicate payment
Procurement and tendering	
Corruption of the procurement process (involving personnel within the entity)	Corruption involving an employee of the entity and a vendor in the selection of a winning bid or tender often involving bribery / kickbacks but often motivated by personal or family association between the bidder and the entity’s employee without direct financial reward – corruption can involve provision of a confidential bid price, contract details or other sensitive information to gain an advantage for one tenderer over other tenderers
Bid rigging (excluding personnel within the entity)	Collusive tendering between multiple bidders for the same contract for mutual advantage (no involvement of the entity’s personnel)

Procurement and tendering	
Conflicts of interest	Undeclared association between an employee of an entity and a tenderer giving rise to an actual or perceived bias in awarding of a contract
Improperly receiving hospitality, gifts and benefits	An employee receiving or soliciting hospitality, gifts or benefits from a vendor or potential vendor hoping to gain a commercial advantage in doing so – depending on the circumstances, this behaviour may constitute fraud
Falsification and manipulation of claims for work-related expenditure	
Use of the entity's funds for personal expenditure	Claiming employee expenses for business-related expenditure not incurred or incurred for personal use or benefit (supported by false or inflated receipts / invoices)
Double-dipping	Claiming multiple reimbursements for the same expenses or claiming for expenses paid personally using receipts for purchases already made via another of the entity's reimbursement systems
Diversion of incoming funds	
Accounts receivable fraud	Redirection of incoming receipts to a spurious account followed by write-off of accounts receivable balance
Unauthorised discounts	Processing unauthorised discounts for early payment of invoices where the discount value is fraudulently transferred to the employee's own bank account
An authorised application of unknown receipts	Funds can be received by an entity where the source of the funds is unknown and the funds are allocated to a suspense account pending rectification – a possible fraud involves the transfer of part of the balance of the suspense account to an employee's own benefit with a manipulation of the accounting system to conceal the theft
Inflating invoice value	Inflating the value of an invoice raised by the entity with receipts in payment of the invoice directed to a spurious account controlled by the staff member concerned who then redirects the correct (reduced) value of the invoice to the entity's correct account
Vendor overpayment	Deliberately overpay a vendor in payment of an invoice for goods or services validly received, claim a refund for the overpayment and then direct the remittance to a spurious bank account
Theft of cash all funds received	Fraudulently failing to record receipt of cash received and then misappropriate for own benefit

Payroll	
Timesheet fraud	Fraudulent submission of falsified timesheets for casual employees who did not work with diversion of resulting remuneration generated to own account
Fraudulent alteration of remuneration rates	Alteration of remuneration rates (salaries or hourly rates) in the payroll system in relation to the employee making the change or for another employee in exchange for personal benefit
Ghost employee fraud	Fabrication of fictitious employees on the payroll with remuneration paid to own account
Fraudulently failing to record personal leave	An employee taking personal leave (annual, long-service, sick or carer's leave) without recording the leave in the HR system
Worker's compensation fraud	Worker's compensation fraud – fraudulent claims for injuries not sustained
Assets and Inventory	
Asset theft	Theft of the entity's assets, including computers and other IT related assets
Information theft	Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans, etc)
Unauthorised private use of employer property	Use of employer property for personal use or benefit
Cash theft	Theft of petty cash
Manipulation of financial reporting	
Fraudulent manipulation of an entity's financial reporting	Fraudulent manipulation of financial reports in order to make it appear that a business entity has performed better (in financial or non-financial terms) than it has actually performed – this can be motivated by a need to demonstrate a certain level of personal performance in order to secure a performance bonus but may also be driven in the public sector by the need to meet political expectations

Cyber-borne attack	
Business email compromise	Emails impersonating vendors or an executive instructing payment to be made to a spurious bank account or a change to existing bank details
Phishing emails	Emails designed to dupe employees into providing personal information (i.e. by clicking on a link or opening an attachment)
Malware	Installing malware onto a computer or computer system within the entity which then issues fraudulent instructions (e.g. to change the bank account of a vendor in the vendor masterfile or change the payroll bank account of one or more employees)

A5.4 Risk treatment tools



A5.4.1 SMART principle for co-designing fraud controls¹⁷

Think about the fraud risk you have described and ways in which you might be able to prevent, monitor or detect the exploitation.

The following table outlines the ‘SMART’ principle which can be applied to help co-design controls with key risk stakeholders.

Specific	The control should have a clear and concise objective. They should also be well defined and clear to anyone with a basic knowledge of the work. Consider: who, what, where, when and why.
Measurable	<p>The control and its progress should be measurable. Consider:</p> <ul style="list-style-type: none"> • What does the completed control look like? • What are the benefits of the control and when they will be achieved? • The cost of the control (both financial and staffing resources).
Achievable	<p>The control should be practical, reasonable and credible and should also consider the available resources. Consider:</p> <ul style="list-style-type: none"> • Is the control achievable with available resources? • Does the control comply with policy and legislation?
Relevant	<p>The control should be relevant to the risk. Consider:</p> <ul style="list-style-type: none"> • Does the control modify the level of risk (through impacting the causes and consequences)? • Is the control compatible with the entity's objectives and priorities?
Timed	The control should specify timeframes for completion and when benefits are expected to be achieved.

¹⁷ Commonwealth Fraud Prevention Centre 'Fraud Risk Assessment – Leading Practice Guide'.

A5.4.2 Example internal controls that may be effective in controlling fraud risks

The following is a short summary of internal controls that experience has shown may be effective in controlling fraud risks in each of the categories contemplated in A5.3.6 above.

Once again, this is not intended as an exhaustive list and is intended to promote consideration of current and possible internal controls within each WA public sector entity when undertaking a targeted fraud risk assessment. It is anticipated that these internal controls may be effective in controlling fraud by:

- preventing a fraudulent transaction from being processed
- quickly detecting a fraudulent transaction after it has been processed thereby preventing any further transactions and minimising loss
- assisting an entity to respond to fraud incidents that have been detected.

The internal controls set out below can be used to:

- identify internal controls already in place during the risk analysis phase of the risk assessment
- identify internal controls that may be useful in further mitigating fraud risk in the risk evaluation phase of the risk assessment.

Accounts payable fraud
• Separate procurement and payment functions
• Separate handling (receipt and deposit) functions from record keeping functions (recording transactions and reconciling accounts)
• Require reconciliation to be completed by an independent person who does not have record keeping responsibilities
• Monitor the entity's financial activity, compare actual to budgeted revenues and expenses
• Require procurement and accounts payable employees to take leave of a minimum duration (e.g. two weeks at a time) with another member of the team performing their role in their absence
• If the entity is so small that duties cannot be separated, require an independent check of work being done supplemented by appropriate and effective data analytics and other reviews appropriate to the entity's situation

Procurement and tendering
<ul style="list-style-type: none"> Implement a tendering / contracting panel made up of independent personnel (i.e. unconnected to the procurement processes), to oversight the awarding of contracts
<ul style="list-style-type: none"> Standard contract conditions and specifications to be used with variations to be approved by senior management
<ul style="list-style-type: none"> Use evaluation criteria as agreed by the contract panel prior to tendering
<ul style="list-style-type: none"> Contract terms and conditions should be those of the purchasing department and not subject to change without the written approval of senior management
<ul style="list-style-type: none"> Clear audit trails with written records including formal authorisation of changes to original documentation
<ul style="list-style-type: none"> Independent post-transactional review of a substantial sample of tendering and contracting transactions with a particular focus on high-risk transaction types
<ul style="list-style-type: none"> Splitting of contacts should not be permitted unless authorised by senior management
<ul style="list-style-type: none"> Management reviews of the reasonableness and competitiveness of prices
<ul style="list-style-type: none"> Ensure contractors with a poor performance record are removed from the approved supplier's list
Falsification and manipulation of claims for work-related expenditure
<ul style="list-style-type: none"> Limit the number of entity issued purchasing cards and users
<ul style="list-style-type: none"> Set account limits with purchasing card providers (value, items that can be purchased etc.)
<ul style="list-style-type: none"> Require employees with entity issued purchasing cards to submit itemised, original receipts for all purchases followed by lodgement of hard copy supporting documentation
<ul style="list-style-type: none"> Independent rigorous examination of credit card transactions each month including detailed review of relevant receipts, invoices and other supporting documentation

Falsification and manipulation of claims for work-related expenditure
<ul style="list-style-type: none"> • Periodic review of a sample of hardcopy supporting documentation • Monitor the entity's financial activity, compare actual to budgeted revenues and expenses • Require an explanation of significant variations from budget
Diversion of incoming receipts
<ul style="list-style-type: none"> • Send official notification to all regular providers / suppliers with particulars of the entity's bank account with statement that this is the only account to which refunds should be remitted • Independent post-transactional view of a sample of invoices rendered to identify any manipulations • Independent post-transactional review of emails between accounts payable / accounts receivable personnel within the entity and customers / clients to determine if there is any indication of manipulation of invoices raised or payments made
Payroll
<ul style="list-style-type: none"> • Payroll system procedures and training • Segregation of duties preventing payroll batch file payments or payroll master file changes without two approvers • Limited system administrator access to the payroll system • System controls to prevent changes to pay rates or salaries without approval • Changes to payroll masterfile (e.g. particularly for bank account numbers) only available to employees via an HR 'kiosk' in the HR system – system unable to process a change of bank account number outside of the HR kiosk • HR system to automatically generate a confirmation email to the employee where there has been a change of masterful data • Rigorous approval process for creation of new employees in the payroll system

Payroll
<ul style="list-style-type: none"> • Timely notification process from HR to Payroll of employees due to resign from the entity
<ul style="list-style-type: none"> • Periodic review of payroll system audit logs
<ul style="list-style-type: none"> • Management review of variance reports from previous payroll run to confirm reasons for significant differences
<ul style="list-style-type: none"> • Employee background checks for new hires with access to the payroll system – this should include criminal record screening and specific questions about any previous integrity concerns / disciplinary findings etc.
<ul style="list-style-type: none"> • Mandatory password changes for those with access to the payroll system to a suitable strength and complexity
<ul style="list-style-type: none"> • Physical security of computers used by payroll staff with direct system access
<ul style="list-style-type: none"> • Electronic timesheet systems and approval process for overtime
Assets and inventory
<ul style="list-style-type: none"> • Physical security of desirable assets (i.e. laptops, IT equipment)
<ul style="list-style-type: none"> • Password protection and remote wiping capability in the case a laptop is lost or stolen
<ul style="list-style-type: none"> • Regular stocktakes of assets and inventory and updating asset registers
<ul style="list-style-type: none"> • Security of cash (i.e. petty cash) and gift vouchers in locked tins or a safe
<ul style="list-style-type: none"> • Tracking systems for assets and approval process for transfer of location
<ul style="list-style-type: none"> • Maintain vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the employee using the vehicle

Manipulation of financial reporting
<ul style="list-style-type: none"> Active engagement with entity's external auditor in relation to the annual audit (i.e. working collaboratively with the auditor to identify any manipulation of the financial reporting)
<ul style="list-style-type: none"> Analysis to identify unusual activity
<ul style="list-style-type: none"> Detailed review of journal and other adjustments to the general Ledger with a focus, as a minimum, on high value transactions
Cyber-borne attack
<ul style="list-style-type: none"> BitLocker protection of all IT assets to ensure security of data
<ul style="list-style-type: none"> Access to databases/systems require unique user logon identification and password authentication
<ul style="list-style-type: none"> Document authorisation that is needed to establish accountability and issue, alter, or revoke user access
<ul style="list-style-type: none"> Prohibit shared user logon IDs and passwords, and user logon IDs and passwords
<ul style="list-style-type: none"> Set database user access permissions that are based on the principles of privilege and separation of duties
<ul style="list-style-type: none"> Restrict access to servers and office locations which contain sensitive and confidential data by physical security to authorised personnel
<ul style="list-style-type: none"> Access to databases/systems require unique user logon identification and password authentication

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
19	Forensic Audit – Construction Training Fund	22 June 2022
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report – Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impacts	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021



**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
F: 08 6557 7600
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au



Western Australian Auditor General's Report



Information Systems Audit Report 2022 – Local Government Entities



Report 22: 2021-22

28 June 2022

**Office of the Auditor General
Western Australia**

Audit team:

Aloha Morrissey
Kamran Aslam
Svetla Alphonso
Ben Goodwin
Khubaib Gondal
Michael Chumak
Sayem Chowdhury
Reshma Vikas
Sooraj Suresh
Tuck Owyong
Karen Telford
Paul Tilbrook
Fareed Bakhsh

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.

© 2022 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Information Systems Audit Report 2022 –
Local Government Entities**

Report 22: 2021-22
June 2022

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

INFORMATION SYSTEM AUDIT REPORT 2022 – LOCAL GOVERNMENT ENTITIES

This report has been prepared for submission to Parliament under the provisions of section 24 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 is the third local government annual information systems audit report by my Office. The report summarises the results of our 2021 annual cycle of information systems audits across a selection of 45 local government entities.

I wish to acknowledge the entities' staff for their cooperation with these audits.

A handwritten signature in black ink, appearing to read 'C Spencer'.

CAROLINE SPENCER
AUDITOR GENERAL
28 June 2022

Contents

Auditor General's overview.....	2
Introduction.....	3
Conclusion.....	4
What we found: General computer controls.....	5
What we found: Capability assessments	6
Information security.....	8
Business continuity.....	11
Management of IT risks.....	12
IT operations	14
Change control.....	15
Physical security	16
Recommendations.....	18

Auditor General's overview

This report summarises important findings and recommendations from our 2020-21 annual cycle of information systems audits at 45 local government entities (entities).

Entities rely on information systems to operate and deliver services to their communities. In doing so, they collect and store vast amounts of information about their residents and operations. As information and cyber security threats continue to evolve, it is increasingly important that entities implement appropriate controls to protect their valuable information and systems. My November 2021 audit report¹ on cyber security highlighted the need for entities to improve their management of cyber security risks and this year's general computer controls (GCC) audits at entities show that information security remains a significant area of concern.

Like last year, none of the 12 entities where we performed capability maturity assessments met our benchmark for information security and none of the entities met our expectations across all 6 control categories. While we saw some improvements in the management of IT risks, physical security and IT operations, change control showed the most progress.

Included in this report are case studies which highlight how weak controls can potentially compromise entities and result in system breaches, loss of sensitive and confidential information and financial loss. Entities need to continuously review and improve their practices to establish robust safeguards and enhance their resilience against cyber threats. Complex networks and systems require smaller entities to also dedicate resources to manage their information and cyber security.

Entities should use the recommendations in this report to address weaknesses in their information systems controls and improve their capability maturity. Given the nature of findings this year, I have chosen again not to identify the audited entities.



¹ Auditor General for Western Australia, [Cyber Security in Local Government](#), Report 9: 2021-22, November 2021.

Introduction

Local government entities (entities) rely on information systems to prepare their financial statements and to deliver a wide range of services to their communities. Our general computer controls (GCC) audits assess if entities have effective system controls in place to support the confidentiality, integrity and availability of their IT systems and financial reporting. These audits are performed as an integral part of, and inform, our financial audit program.

This report summarises the GCC audit findings reported to 45 entities for 2020-21. For 12 of these entities, generally medium to large, we also performed capability maturity assessments. A GCC audit with a capability maturity assessment is the most comprehensive information systems audit we undertake. We use these findings to inform our financial audit risk assessment and work program for the sector.

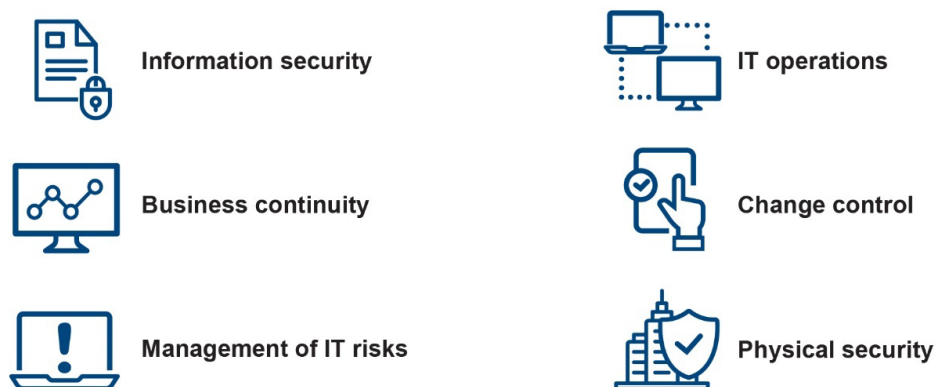
For our capability maturity assessments, we asked the 12 entities to self-assess against the provided capability maturity model. We then compared their results to ours (which were based on the results of our GCC audits). These assessments are a way to see how well-developed and capable entities' established IT controls are.

For the remaining 33 entities, our contract audit firms or our financial audit teams examined the GCCs but did not undertake capability maturity assessments. Information system findings identified during these audits are included in this report.

The methodology we have developed for our GCC audits is based on accepted industry good practice. Our assessment is also influenced by various factors including:

- business objectives of the entity
- level of dependence on IT
- technological sophistication of computer systems
- value of information managed by the entity.

We focused on the following 6 categories (Figure 1) for both our GCCs and capability maturity assessments.



Source: OAG

Figure 1: GCC categories

Throughout the report we have included case studies that illustrate the significant impact poor controls can have on entities.

Conclusion

We reported 358 control weaknesses to 45 entities this year, compared to 328 weaknesses at 50 entities last year. Ten percent (37) of this year's weaknesses were rated as significant and 71% (254) as moderate. These weaknesses represent a considerable risk to the confidentiality, integrity and availability of entities' information systems and need prompt resolution.

Fifty-six percent (202) of the findings were unresolved issues from last year. Entities need to address these weaknesses to reduce the risk of their systems and information being compromised.

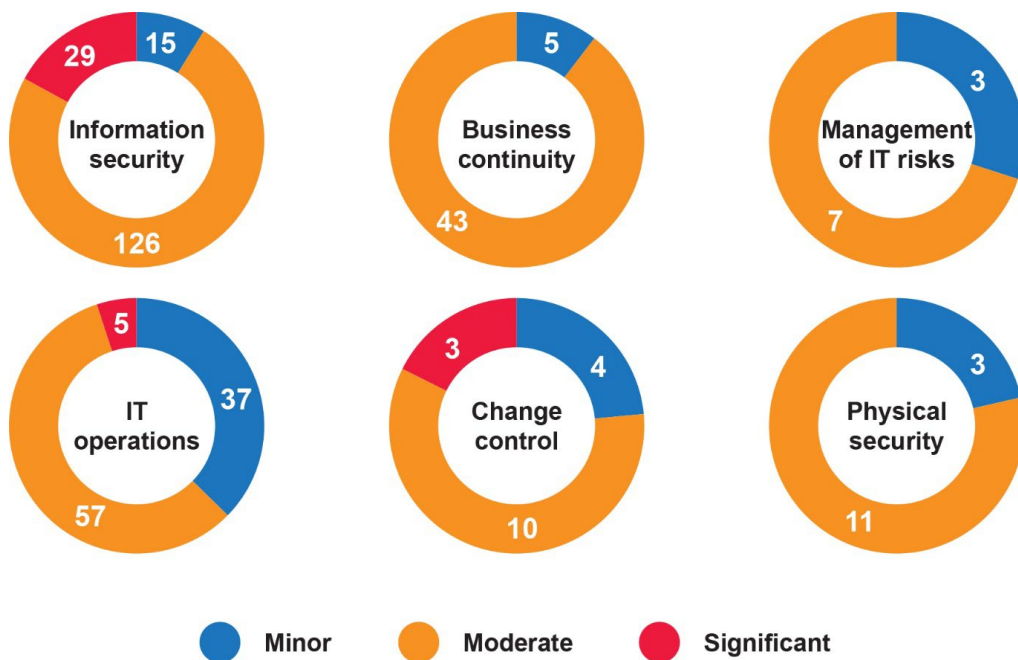
None of the 12 entities that had capability maturity assessments met our expectations across all 6 control categories, a similar finding to last year. Information security remains a significant risk again this year and needs urgent attention. Compared to 2019-20, there have been some improvements in change control, management of IT risks, physical security and IT operations. However, entities need to improve in all 6 control categories.

What we found: General computer controls

In 2020-21, we reported 358 findings to the 45 entities we audited. We reported the weaknesses we found to each entity in a management letter. As management letters are often made public, we removed any sensitive technical details which could increase an entity’s risk of cyber attacks. To assist entities to address weaknesses we reported these sensitive details to them in separate confidential letters. Entities generally agreed to implement our recommendations.

Figure 2 summarises the distribution and significance of our findings across the 6 control categories.

Like last year, we rated most of our findings as moderate. Entities that fail to address these moderate risks can, over time, become more exposed to vulnerabilities. We have included in this report specific case studies to highlight how weak controls can potentially compromise entities’ systems.



Source: OAG

Figure 2: Distribution and significance of GCC findings in each control category

What we found: Capability assessments

We conducted in-depth capability maturity assessments at 12 entities. We used a 0 to 5 rating scale² (Figure 3) to evaluate each entity’s capability maturity in each of the 6 GCC categories. Our model allows us to compare entity results from year to year. We expect entities to achieve a level 3 (Defined) rating or better across all 6 categories.

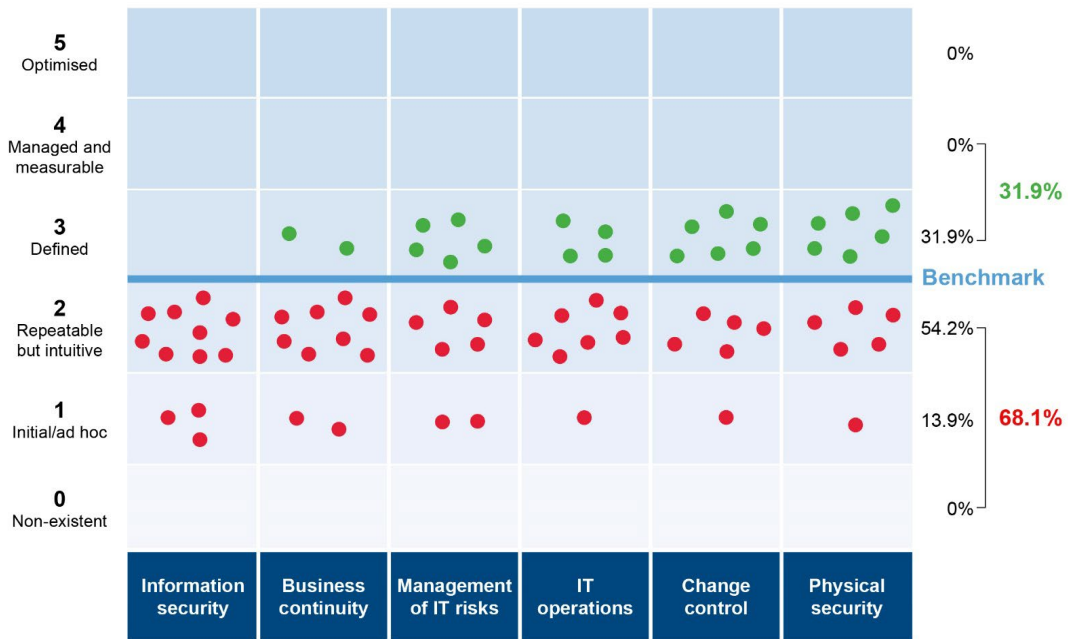


Source: OAG

Figure 3: Rating scale and criteria

Figure 4 shows the results of our capability assessments across all 6 control categories for the 12 entities we assessed in 2020-21.

² The information within this maturity model assessment is derived from the criteria defined within COBIT 4.1, released in 2007 by ISACA.



Source: OAG

Figure 4: 2020-21 capability maturity model assessment results

The percentage of entities rated level 3 or above for individual categories was as follows:

Category	2020-21 %	Change	2019-20 %
Information security	0	—	0
Business continuity	17	↓	18
Management of IT risks	42	↑	27
IT operations	33	↑	18
Change control	50	↑	18
Physical security	50	↑	45

Source: OAG

Table 1: Percentage of entities rated level 3 or above

None of the 12 entities met our expected benchmark (level 3 Defined) across all control categories.

There were some improvements in the management of IT risks, IT operations, change control and physical security, however, most entities still fell below our benchmark. Information security remains a significant concern, with all entities below our benchmark and not able to demonstrate adequate controls. A lack of robust controls can expose entities and impact critical services provided to the public.

Information security

Cyber intrusions are becoming more sophisticated and frequent. Transitioning to digital services to achieve efficiencies increases the risk profile of many entities. Protection of sensitive and critical information that entities hold within their financial and operational systems should be managed with the highest priority using better practice information security controls to mitigate risks.

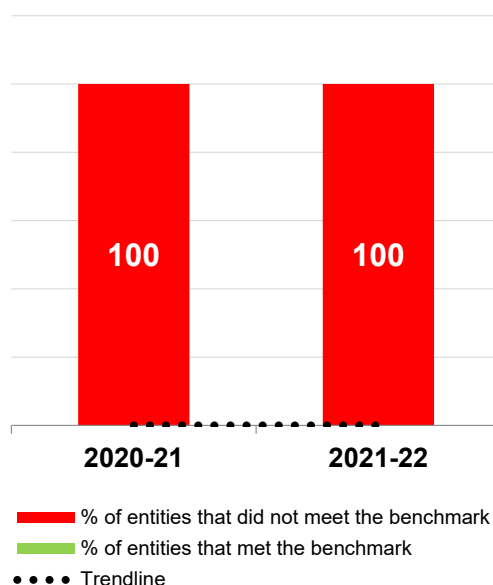
Our GCC audits and capability maturity assessments assess against better practice controls for information and cyber security. Figure 5 lists some of these controls.



Source: OAG

Figure 5: Information security – Better practice controls

None of the 12 entities met our benchmark for information security either because they did not have documented policies, processes and controls or they were not effective (Figure 6). Entities have a responsibility to implement adequate and robust controls to protect key systems and information.



Source: OAG

Figure 6: Information security – percentage of entities that met/did not meet our benchmark


Common weaknesses we found included:

- **Inadequate information and cyber security policies** – policies did not sufficiently cover key areas of information and cyber security or were out of date.
- **Multifactor authentication not used** – a number of systems did not have multifactor authentication to strengthen access.
- **Administrator privileges not managed well** – administrators did not have separate unprivileged accounts for normal day to day tasks. Limiting privileges and separating administrative accounts are important mitigations against network and system compromise.
- **Vulnerability management is not effective** – entities did not have appropriate processes to identify and address vulnerabilities, which increases the risk of compromise.
- **Network segregation not appropriate** – networks were not segregated to limit and contain the impact of a compromise. Partitioning the network into smaller zones and limiting the communication between these zones is an important control.
- **Unauthorised device connectivity** – there are a lack of controls to detect or prevent unauthorised devices from connecting to entity internal networks. These devices can serve as an attack point and spread malware or listen in on network traffic.
- **Emails not protected** – entities did not have controls to ensure the integrity and authenticity of emails to reduce the likelihood of successful phishing attacks. Controls such as domain-based message authentication reporting and conformance (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented to prevent email impersonation.

- **Lack of data loss prevention controls** – no processes to detect or block unauthorised transfers of sensitive data outside of the entities.

The importance and potential impact of common information and cyber security weaknesses are illustrated in the following case studies.

Case study 1: No policy to manage information and cyber security




Information security policy

One entity did not have a policy to manage cyber and information security. This means, systems or services may not meet security expectations of senior management and the entity may fail to achieve its objectives.

Adequate and clear policies are needed to ensure the security of information systems.

Case study 2: Weak password results in a network compromise




Password

One entity experienced a security breach when a cybercriminal was able to guess a weak password on an account used to access a public facing server through remote desktop protocol (RDP). A lack of network segregation allowed the attacker to access other parts of the network, gain privileged access to the domain controller and maliciously encrypt servers and information.

The use of strong password/passphrases, network segregation and multi-factor authentication reduce the risk of compromise.

Case study 3: No controls to mitigate malware infections



Malware protection

One entity had anti-malware protection installed on some servers but not others. It did not have application whitelisting and blocking in place or only allow trusted macros. These controls prevent delivery and execution of malicious programs.

Without appropriate controls to protect systems against malware, there is an increased risk of compromise to the confidentiality, integrity and availability of entity information or data.

Case study 4: Default domain administrator account is not controlled



Limit admin privilege

One entity shared the highly privileged default domain administrator account with individuals in different business units and had not changed the account password since 2005. The account was also heavily used for day to day operations and services, instead of using separate dedicated service accounts.

Inappropriate management of the account increases the risk that the entity will not be able to hold individuals to account for unauthorised modifications to its systems and information.

Case study 5: Poor management of technical vulnerabilities

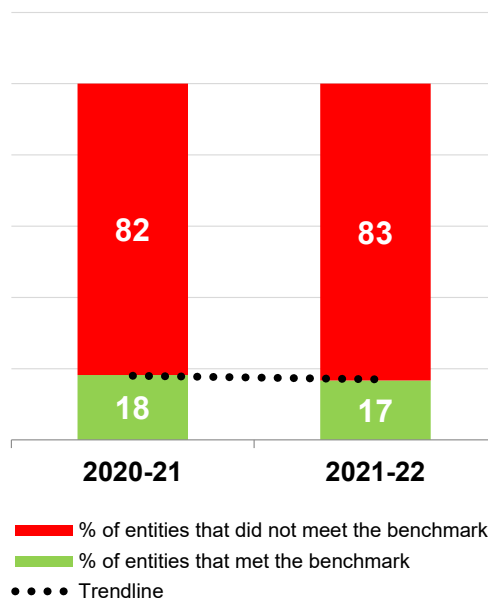


An audited entity did not have a process to manage technical vulnerabilities and system currency. It had not tested the adequacy of its external network controls to detect and prevent cyber attacks. Its process to apply software patches was also not operating well as we identified critical and high severity vulnerabilities dating back to 2013 that had not been patched.

Without effective procedures and processes to manage technical vulnerabilities in a timely manner, entities leave their IT systems exposed to malicious attackers. This could result in unauthorised access and system compromise.

Business continuity

There was no material change from last year with only 2 of the 12 entities (17%) meeting our benchmark in this category (Figure 7). Business continuity and disaster recovery plans help entities to promptly restore key business functions and processes during or after an unplanned disruption. Without these plans, entities could suffer extended outages and disruption to the delivery of important services to their communities.



Source: OAG

Figure 7: Business continuity – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Lack of business continuity and disaster recovery plans** – entities did not have appropriate business continuity and disaster recovery plans, or they were out-of-date.
- **Disaster recovery plans not tested** – without appropriate testing of disaster recovery plans, entities cannot be certain the plan will work when needed.

Documented up-to-date business continuity and disaster recovery plans help entities to promptly recover critical information systems in the event of an unplanned disruption to their operations and services. The plans should identify critical business functions and IT systems along with their recovery time objectives.

The effectiveness of these plans should be periodically tested to identify improvements where required. Tests can also be used to check that key staff are familiar with the plans and their specific roles and responsibilities in a disaster situation.

The following case study illustrates common weaknesses in recovery procedures.

Case study 6: Configuration backups are not performed



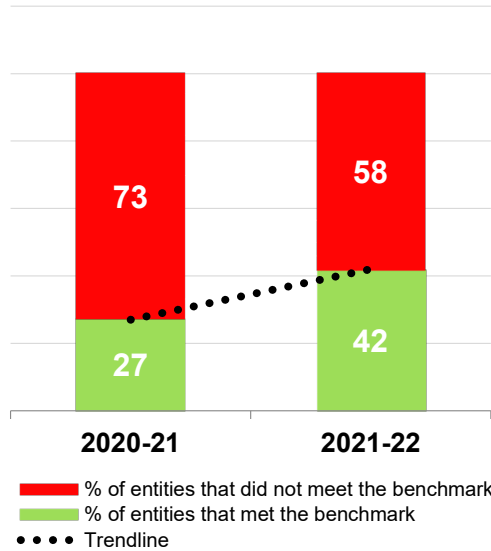
An audited entity did not backup the configuration of its firewall which protects its network from cyber attacks. In the event of an emergency, the entity may not be able to recover its firewall in a timely manner, which will impact delivery of services and security of its network.

**Configuration
backups**

Management of IT risks

Forty-two percent of entities met our benchmark for this category in 2020-21, compared to 27% last year (Figure 8).

Entities should be aware of information and cyber security risks associated with IT including operational, strategic and project risks. All entities should have risk management policies and processes to assess, prioritise, address and monitor the risks that affect key business objectives.



Source: OAG

Figure 8: Management of IT risks – percentage of entities that met/did not meet our benchmark


Common weaknesses we found included:

- **Out-of-date policies and processes to identify, assess and treat IT risks** – without appropriate policies and processes entities cannot effectively manage their IT risks.
- **Inadequate risk registers** – risk registers did not record controls and treatment action plans and risk ratings were not appropriately assessed.

Without IT risk management policies and practices to identify, mitigate and manage threats within reasonable timeframes, entities may not meet their business objectives to deliver key services to their communities.

The following case study illustrates that entities need processes to identify their risks.

Case study 7: Entity is not aware of its information and cyber risks



An audited entity maintained other corporate and financial risks, but it did not have a process to identify and address its cyber security risks.

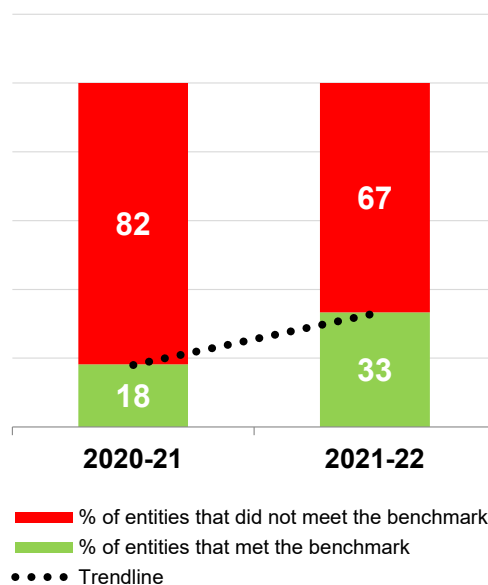
The entity is at an increased risk of information and cyber security breaches.

Information and cyber security risk management

IT operations

Entities improved in this category with 33% meeting our benchmark in 2020-21 (Figure 9). However, we identified similar weaknesses to those highlighted in last year’s report.

IT operations maintain and support the delivery of entity services. Clearly defined and effectively managed IT operations support IT infrastructure that can withstand and recover from errors and failures.



Source: OAG


Figure 9: IT operations – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Processes are not defined** – a lack of or out of date procedures to support day to day operations, such as incident and problem management.
- **Inadequate monitoring of events** – entities did not have policies and procedures to monitor event logs. System logs provide an opportunity to detect suspicious or malicious behaviour in key business applications.
- **Supplier performance not monitored** – supplier performance was not reviewed to identify and manage instances of non-compliance with agreed service levels.
- **Background checks for new starters were not performed** – staff in privileged IT positions did not go through background checks (e.g. police clearance).
- **Access was not reviewed** – regular checks were not done to validate users had the level of access to systems applicable to their role or function, and revoke user access upon termination.

The following case study illustrates a common weakness in IT operations.

Case study 8: Contractor access was not revoked in a timely manner



User account management

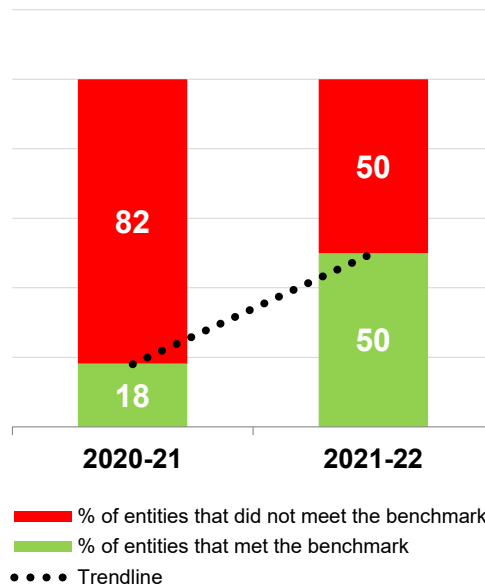
One entity did not have a central record of contract staff and therefore could not easily assess if their network access was appropriate. We sampled 13 active accounts and found that 8 belonged to terminated contract staff who no longer worked with the entity.

Poor processes to manage contract staff increases the risk of unauthorised access to the entity’s IT systems and information.

Change control

Fifty percent of entities met our benchmark in 2020-21 (Figure 10), the largest improvement across the 6 control categories. This is 1 of the 2 categories where at least half of the entities met the benchmark and it is pleasing to see significant year on year improvement.

We reviewed entities’ approaches to managing IT changes to minimise the risks and impacts to stakeholders. We covered change authorisation, testing, implementation and outcomes. An overarching change control framework ensures changes are made consistently and reliably.



Source: OAG

Figure 10: Change control – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Change processes not followed** – changes to critical systems did not follow change procedures. If formal procedures are not followed, there is a risk changes may be applied inconsistently resulting in unplanned system downtime and interruption to critical services.

- **Change management processes not documented** – without documented processes, changes made to IT infrastructure can adversely affect entities' operations leading to unplanned or excessive system downtime.
- **Changes were not assessed prior to implementation** – allowing significant changes without appropriate scrutiny or approval increases the risk of system outages.

Without appropriate change control, entities risk compromising the integrity of their systems and information. This can lead to excessive outages and downtime to key systems and impact their delivery of services.

The following case study illustrates the risks when IT changes are not controlled and monitored.

Case study 9: Poor change management practices could result in financial system instability



Change management

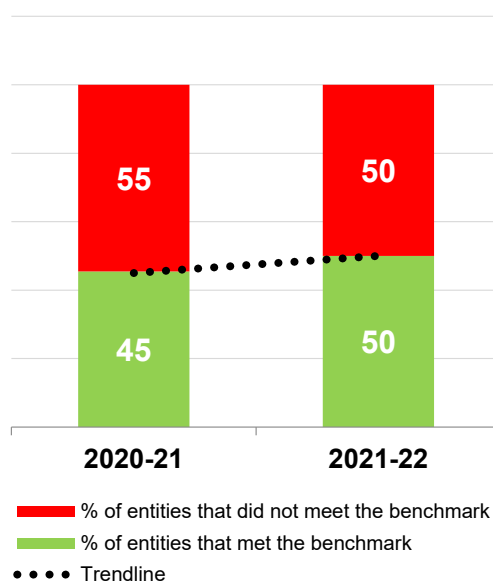
One entity made changes to its financial system without testing the impact on system integrity and availability in an independent test environment. Uncontrolled changes can have significant unintended consequences to systems and the delivery of key services.

These changes were also not recorded, contrary to the entity's change management policy. Failure to record changes increases the effort required to respond, recover and restore business as usual operations.

Physical security

There was a small improvement in physical security with half the entities meeting our benchmark this year (Figure 11).

IT systems are housed in purpose-built server rooms, which must have restricted access and adequate cooling and power. We reviewed if IT systems were protected against potential environmental hazards and tested access restrictions to ensure only authorised individuals could access the server rooms.



Source: OAG

Figure 11: Physical security – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Combustible and non-essential items were stored in server rooms** – the risk of outages is higher if server rooms are not appropriately maintained.
- **Unnecessary access to server rooms** – staff and contractors were assigned access to server rooms that they did not require and visitor access to server rooms was not logged. Lack of controlled access increases the risk of system outages and compromise from unauthorised access.
- **Fire suppression systems were not installed** – without appropriate fire suppression systems, IT infrastructure is likely to be damaged in the event of a fire.

The following case study illustrates the risk of server room outages if not protected against physical and environmental hazards.

Case study 10: Poor management of server rooms



Physical security

One entity stored combustible materials such as furniture and cardboard boxes in their server room. In addition, an excessive number (114) of people had access to the server room and a visitor log was not maintained.

There is an increased risk of accidental or deliberate damage and unauthorised access to systems.

Recommendations

1. Information security

- a. Senior executives should implement appropriate policies and procedures to ensure the security of information systems and support their entity business objectives.
- b. Management should ensure good security policies and practices are implemented and continuously monitored for control areas identified in Figure 5, including:
 - i) patching and vulnerability management
 - ii) application hardening and control
 - iii) implement technical controls to prevent impersonation and detect/prevent phishing emails
 - iv) strong passphrases/passwords and multi-factor authentication
 - v) limit and control administrator privileges
 - vi) segregate network and prevent unauthorised devices
 - vii) secure cloud infrastructure, databases, email and storage, and know clearly 'who' they are handing entity and citizen data to through their use of cloud services
 - viii) cyber security monitoring, intrusion detection and protection from malware.

2. Business continuity

Entities should have appropriate business continuity, disaster recovery and incident response plans to protect critical systems from disruptive events. These plans should be periodically tested.

3. Management of IT risks

Entities should:

- a. understand their information assets and apply controls based on their value
- b. ensure IT risks are identified, assessed and treated within appropriate timeframes. Senior executives should have oversight of information and cyber security risks.

4. IT operations

Entities should implement policies and procedures to guide key areas of IT operations such as incident management and supplier performance monitoring.

5. Change control

Approved change control processes should be consistently applied when making changes to IT systems. All changes should go through planning and impact assessment to minimise the occurrence of problems. Change control documentation should be current and approved changes formally tracked.

6. Physical security

Entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access, or accidental or environmental damage to IT infrastructure and systems.

Under section 7.12A of the *Local Government Act 1995*, the 45 audited entities are required to prepare an action plan to address significant matters relevant to their entity for submission to the Minister for Local Government within 3 months of this report being tabled in Parliament, and for publication on the entity's website. This action plan should address the points above, to the extent that they are relevant to their entity.

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
21	Delivering School Psychology Services	23 June 2022
20	Fraud Risk Management - Better Practice Guide	22 June 2022
19	Forensic Audit – Construction Training Fund	22 June 2022
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impact	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021



**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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



Office of the Auditor General for
Western Australia



Report 5: 2022-23 | 17 August 2022

FINANCIAL AUDIT RESULTS

Local Government 2020-21



**Office of the Auditor General
Western Australia**

Audit team:

Grant Robinson
Lyndsay Fairclough
Financial 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.

© 2022 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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: Tyler Olson/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Financial Audit Results –
Local Government 2020-21**

Report 5: 2022-23
17 August 2022

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

FINANCIAL AUDIT RESULTS – LOCAL GOVERNMENT 2020-21

Under section 24 of the *Auditor General Act 2006*, this report covers the final year of a four year transition for my Office to conduct the annual financial audits of the local government sector, following proclamation of the *Local Government Amendment (Auditing) Act 2017*.

This report on the 2020-21 financial audits of 132 of the applicable 148 local government entities includes:

- results of the audits of local government entities' annual financial reports and their compliance with applicable legislation for the financial year ending 30 June 2021
- issues identified during these annual audits that are significant enough to bring to the attention of the Parliament.

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
17 August 2022

Contents

Auditor General's overview.....	7
Executive summary	8
Review of the four-year transition.....	8
Introduction	10
Year at a glance	11
Recommendations.....	13
Timeliness and quality of financial reporting.....	14
Reporting requirements.....	14
Review of financial reports submitted for audit	14
Recommendation	16
Summary of audit opinions	17
Two disclaimers of opinion for 2019-20	17
Response from Shire of Yalgoo.....	18
Two qualified audit opinions for 2020-21	18
Twenty-four entities received emphasis of matter paragraphs.....	18
Seventy-five entities had 193 material matters of non-compliance with legislation	19
Adverse trends in the financial position of 109 entities	20
We issued 275 audit certifications	20
Control weaknesses	22
Management controls.....	22
Recommendation	27
Information system controls.....	28
Issues impacting entity reporting	29
Rehabilitation of landfill sites	29
Recommendation	30
Valuation of assets.....	30
Developer contributions – Accounting for cash in lieu of public open space	31
Implementation of Service Concession Grantors Standard AASB 1059	32
Other changes to accounting standards	33

Impact of emergencies	34
COVID-19	34
Cyclone Seroja.....	37
Opportunities for the DLGSC to improve the efficiency of financial reporting	38
Quality and timeliness	38
Response from the DLGSC.....	39
Review of financial ratios.....	39
Response from the DLGSC.....	40
Reduced disclosure reporting by entities	40
Response from the DLGSC.....	41
Local Government Regulations Amendment (Financial Management and Audit) Regulations 2022	41
Recommendation	41
Appendix 1: Status and timeliness of 2020-21 audits	42
Appendix 2: 2019-20 disclaimers of opinion	48
Appendix 3: 2020-21 qualified opinions	49
Appendix 4: Emphasis of matter paragraphs included in auditor's reports	50
Appendix 5: Material matters of non-compliance with legislation.....	54
Appendix 6: Certifications issued.....	57
Appendix 7: Other opinions and certifications issued since 18 November 2021	62

Auditor General's overview

The 2020-21 financial year marked the end of a four-year transition of local government financial auditing to my Office. The transition has brought many challenges as local governments and regional councils (entities) adjusted to our robust audits and we have learnt about the intricacies of the sector. Despite the challenges, it has been rewarding to facilitate financial reporting improvements and increase transparency of this important layer of government which impacts all West Australians. I have included a brief review of the transition at the beginning of this report.



For the 2020-21 audit cycle, we have completed 132 of 148 audits by 30 June 2022, with 16 outstanding. We have seen a demonstrated effort by the sector to improve the quality and timeliness of their annual financial reports and pleasingly reported a 15% decrease in weaknesses in financial management controls. This follows a 12% decrease the year before. To see this reduction in management control issues, across a larger number of audited entities, shows a comprehensive response by the sector to improve their current practices and strengthen the integrity of their financial reporting environment.

However, two entities received a qualified opinion on their financial reports and there may be further qualifications on the opinions not yet issued. We also reported a higher rate of material non-compliance and information system control weaknesses than previously.

In this report I have also included previously unreported outstanding opinions from 2019-20 for the Shires of Wiluna and Yalgoo. For both entities I issued a disclaimer of opinion as I was unable to obtain sufficient appropriate audit evidence on their books and records because of deficiencies in their internal controls and record keeping. A disclaimer of opinion is a serious matter for my Office as there is a missed opportunity for assurance over financial accountability and continuous improvement. This leads to a lack of confidence in the appropriate use of public monies.

To support continuous improvement in the local government sector, I encourage entities to review the findings of their audits, as well as this audit results report. Each entity should consider our recommendations in the context of their own operating environments and governance frameworks.

I note the newfound willingness and leadership of the Department of Local Government, Sport and Cultural Industries to enhance financial reporting, reduce complexity and cost, and enable improved governance for the sector. This report also outlines its progress on our previous recommendations.

Finally, I wish to acknowledge my incredibly hardworking staff, our contract audit firm partners and staff in the audited entities for their dedication to this year's audit process. Your professionalism and cooperation in working through uncommon challenges to complete the audits is appreciated.

Executive summary

Review of the four-year transition

The 2020-21 financial audit was the first year the Auditor General had responsibility for all 148 local government audits, marking the end of the four-year transition provided in the *Local Government Amendment (Auditing) Act 2017*.

A challenging transition

The transition has not been easy for the Office of the Auditor General (OAG) or entities, but Parliament was correct to acknowledge that change and improvement was needed for the sector. In too many cases, the quality of both financial reporting and audit was not what ratepayers and communities would rightly expect.

Our audits have brought greater rigour, scrutiny and sector-wide oversight. While challenging for many local governments and regional councils (entities), they have responded positively, particularly when they have understood that this helps them provide better transparency, accountability and financial management.

How challenging entities have found it to adapt to our requirements and approach was not predictable. Many smaller entities, who we might have expected to struggle, have adapted relatively easily while some of the larger ones with greater capacity have found it difficult. This has been particularly interesting given that all entities, regardless of size and complexity have to comply with the same legislative and regulatory framework.

Setting the baseline

As is often the case, the initial stages of reform have revealed many of the issues that need fixing. For the local government sector this includes the quality and timeliness of financial reporting and the need to aim for better practice, not just meet minimum levels of compliance. Our office has prepared guidance on preparing financial statements¹ and other topics² which entities have been encouraged to use.

Achieving consistency in some key areas underpins ongoing improvement. One area we continue to report on each year³ is inconsistencies in property and asset valuation methodologies. Entities can see significant valuation swings depending on the valuer they appoint and the assumptions the valuer makes. While regulation changes mean a formal valuation is no longer required each year, entities still need to ensure their assets are recorded at fair value. Forthcoming guidance from the Australian Accounting Standards Board and in turn the Department of Local Government, Sport and Cultural Industries (DLGSC) may help.

Through the transition we have come to understand much better the extent of reporting and compliance required of entities, in some cases exceeding that required of the State government sector. We have advocated to, and worked with, the DLGSC for a reduction in these requirements and are pleased new model financial statements, with decreased reporting but without a loss of key disclosures, will be available for entities in 2022-23. We will continue to liaise with the DLGSC on other proposed reforms that aim to increase accountability, transparency and efficiency for the sector.

¹ Office of the Auditor General, [Western Australian Public Sector Financial Statements – Better Practice Guide](#), OAG, Perth, 2021.

² Office of the Auditor General, [‘Better Practice Guidance’](#), OAG, accessed August 2022.

³ Office of the Auditor General, [Audit Results Report – Annual 2017-18 Financial Audits of Local Government Entities](#), OAG, Perth, 2019, p. 20.

The transition has also identified areas of improvement for our Office. Specifically, we have had to increase the training of our employees and contract audit firms to adequately understand the local government environment, which differs in some significant ways to the State and tertiary sectors. We also intend to increase the time our auditors spend onsite to further improve the engagement, efficiency and timeliness of audits.

We are also determined not to allow any overruns from our State sector audits to impact our delivery of local government audits, as it did for the 2020-21 audit cycle (due to a record number of State government entity audit qualifications). This means if State entities are not audit-ready or we encounter delays undertaking their audits, our teams will move on to the local government program as scheduled, even if State entities are not finalised. Our resolve on this matter will be tested during the 2021-22 audits, but we look forward to reporting back to the Parliament and all our audited entities on how this approach unfolds.

Seeing results

While the timeliness and quality of annual financial reports have been significant issues through the transition, there are signs of improvement. The reduction since 2018-19 in financial management control weaknesses shows a clear effort by entities to improve their current practices and strengthen the integrity of their financial reporting environment. Although the upward trend in material matters on non-compliance indicates there is still improvement needed. The following table shows entities' audit results over the past four years.

Audit year	2017-18	2018-19	2019-20	2020-21
Number of entities subject to OAG audit	46	112	132	148
Clear audit opinions	44	107	129	130*
Qualified opinions	2	5	1	2*
Disclaimers of opinion	0	0	2	0*
Material matters of non-compliance	36	93	101	193*
Management control issues	198	802	704	601*

Source: OAG

* Some 2020-21 audits are still ongoing and therefore these results are for 132 entities only.

Table 1: Audit results for four year transition period

Understanding of the significant role of audit committees in the annual reporting and audit process has also improved. Better informed and active audit committees are now more suitably equipped to quality review the financial report and assess the accountability and integrity of entities' reporting, control environment and risk management practices.

Where to from here

There is still a long way to go but we are committed to working with entities, the DLGSC and sector associations⁴ to continue improving the sector and our own processes to aid timely reporting to the community and Parliament.

From the 2021-22 financial year audits we will recognise the top entities who demonstrate best practice in the sector, as we do for the State and tertiary sectors. Our best practice assessment criteria include:

⁴ Western Australian Local Government Association (WALGA) and Local Government Professionals Australia WA.

- clear opinions on financial reports and controls
- the number and significance of control weaknesses raised in management letters
- good quality financial reports, supported by reliable working papers and submitted for audit within the agreed timeframe
- management resolution of accounting standards and presentation issues
- availability of key staff during the audit process.

For 2020-21, OAG staff performed 21 audits in-house, with the other 127 performed by contract audit firms on our behalf. We expect to increase the number of audits we perform in-house over time. However, a large proportion will continue to be performed by our accredited contract audit firms. These are periodically re-tendered to provide open and fair competition and to ensure value for money.

Introduction

This report contains findings from our 2020-21 financial audits of the local government sector. It includes the results for 132 of the 148 entities (Appendix 1), with the remaining 16 entities' results to be tabled in Parliament once their audits are completed.

Our annual financial audits focus on providing assurance over an entity's financial report. The Auditor General provides an opinion on the report which can be:

- clear – this indicates satisfactory financial controls and that the financial report is based on proper accounts, presented fairly, complies with relevant legislation and applicable accounting standards, and fairly represents performance during the year and the financial position at year end
- clear with an emphasis of matter – this brings attention to a matter disclosed in the entity's financial report but is not significant enough to warrant a qualified opinion
- qualified – these opinions are given when the audit identifies that the financial report is likely to be misleading to users, controls were inadequate or there was a material conflict with applicable financial reporting frameworks
- disclaimer of opinion – issued when the auditor is unable to form an opinion due to insufficient evidence being available. This is the most serious audit opinion and is only issued after we have exhausted our efforts to achieve the desired audit objectives.

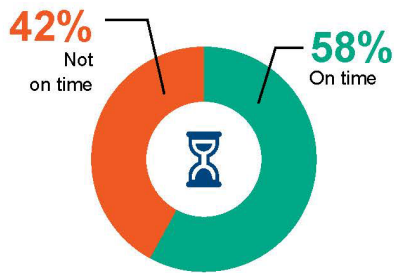
During an audit we also make recommendations to entities on relevant matters of compliance, financial management and information system controls. A summary of our findings is included in this report.

Also included are matters we have noted which have or may impact an entity's financial report. This year this includes how entities account for the rehabilitation of landfill sites, changes to the accounting treatment for cash in lieu of public open space from developer contributions, inconsistencies in how entities value assets and changes to accounting standards.

The appendix includes other opinions and certifications issued for the State government sector since 18 November 2021.

Year at a glance

Auditing local government



Audits completed by 31 December



148 local government entities



132 audits finalised and the results included in this report



21 entities audited by OAG staff



127 entities audited by contracted audit firms



The 132 entities with finalised audits had:

\$45 billion of total reported assets



\$3.8 billion in total operating revenue

2.2 billion in rates

\$958 million in fees and charges

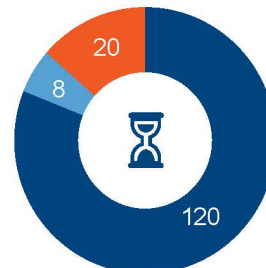
Quality and timeliness of financial reports (page 14)

Quality

Roughly half of the entities submitted financial statements for audit that were of a reasonable standard and required minimal revisions or adjustments. However, the remaining half were found to have numerous errors and disclosure requirements were unmet.

Timeliness

- Submitted to OAG by 30 September
- Received an extension and met deadline
- Did not meet 30 September or extension deadline



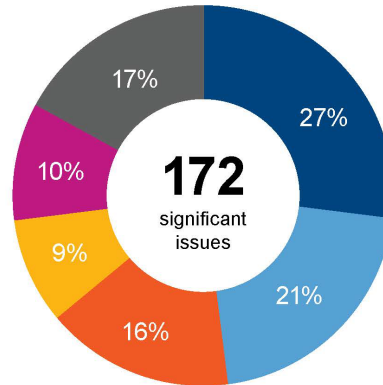
Audit results



601 management control issues
(page 22)

During 2020-21, we alerted 126 entities to control weaknesses that needed their attention. One hundred and seventy-two were rated as significant, 359 moderate and 70 minor.

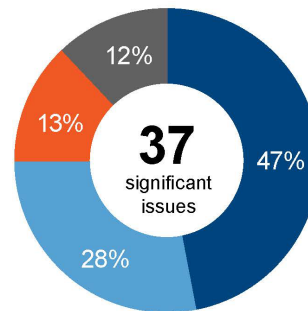
- Expenditure
- Financial management
- Payroll and human resources
- Asset management
- Revenue
- Other



193 Material matters of non compliance with legislation (page 19)



358 information system control weaknesses (page 28)



- Information security
- IT operations
- Business continuity
- Other

Issues impacting entity reporting



Rehabilitation of landfill sites (page 29)



Valuation of assets (page 30)



Developer contributions – Accounting for cash in lieu of public open space (page 31)



Accounting standard changes (page 32)

Recommendations

1. We encourage entities to make use of our *WA Public Sector Financial Statements – Better Practice Guide* (available at audit.wa.gov.au) to improve their financial management and reporting practices, processes and procedures (page 16).
2. Local government entities should ensure they maintain the integrity of their financial control environment by:
 - a. periodically reviewing and updating all financial, asset, human resources, governance, information systems and other management policies and procedures and communicating these to staff
 - b. conducting ongoing reviews and improvement of internal control systems in response to regular risk assessments
 - c. regularly monitoring compliance with relevant legislation
 - d. promptly addressing control weaknesses brought to their attention by our audits and other audit and review mechanisms
 - e. ensuring they consider new and revised accounting standards for their impact on financial operations to prepare a compliant financial report at year end (page 27).
3. The Department of Local Government, Sport and Cultural Industries should provide guidance to assist entities with understanding the requirements of and interpreting the Australian Accounting Standards Board (AASB) accounting requirements to ensure greater accounting consistency across the sector, including recognising provisions for the rehabilitation of landfills and other contaminated sites (page 30).
4. The Department of Local Government, Sport and Cultural Industries should continue to work with local government stakeholders towards the introduction of model financial statements for the 2022-23 financial year (page 41).

Timeliness and quality of financial reporting

Reporting requirements

Each entity is required to prepare an annual financial report that includes:

- a Statement of Financial Position, Statement of Comprehensive Income by Nature or Type, Statement of Comprehensive Income by Program, Statement of Changes in Equity and Statement of Cash Flows
- a Rate Setting Statement
- seven financial ratios required under section 50(1) of the Local Government (Financial Management) Regulations 1996 (FM Regulations)
- other note disclosures such as trading undertakings and major land transactions.

We have previously recognised that the quantity of detail reported in some aspects is onerous and exceeds that reported by most Western Australian (WA) State government entities and by local governments in other jurisdictions. From page 38 we have summarised DLGSC's progress with some reforms in this regard including the recent changes to the Local Government Regulations Amendment (Financial Management and Audit) Regulations 2022, gazetted on 17 June 2022.

Review of financial reports submitted for audit

Timeliness

Under section 6.4(3) of the *Local Government Act 1995* (LG Act), entities must submit their annual financial reports to the OAG for audit by the statutory deadline of 30 September. Of the 148 entities:

- 120 met the 30 September deadline
- 13 did not
- 17 received approval from the Minister to extend their submission deadline, of these:
 - 8 met the extended deadline
 - 7 did not
 - 2 did not require the extension as they met the 30 September deadline and are included in the 120 figure above.

Further details of entities' timeliness are provided in Appendix 1. Failure to provide good quality financial statements in a timely manner causes delays in the start and therefore the finalisation of audits.

We completed 86 of 148 audits (58%) by 31 December 2021 (compared to 65 of 132 audits (49%) by the same time last year) as required by section 7.9 of the LG Act. While this is an improvement from the previous year, we again encountered issues with the quality and timeliness of information provided by entities. Some entities experienced problems with insufficient evidence to support the financial report and numerous errors requiring correction. We also noted resourcing constraints impacting the sector, most notably in regional entities, which undoubtedly added to the challenge. Finally, we acknowledge the impact of delayed audit completions in numerous State sector entities on our ability to commence some local government entity audits.

Quality

We rate the quality of entities' financial statements that they submit for audit. Roughly half had statements that were of a reasonable standard and required minimal revisions or adjustments.

However, the remaining entities:

- had poor record keeping practices which delayed providing the necessary information for audit
- had numerous errors in their financial statements and disclosure requirements were not met
- experienced finance staff turnover and attrition during crucial times in the financial year, or key personnel were not available to respond to the auditors at key times as they had taken leave.

We identified numerous errors that were corrected by the entities during the audit process. These errors included:

- incorrect valuation method used
- incorrect revenue recognition of funds received in advance
- bank reconciliations for the municipal account not reconciled, resulting in back dated payments not being identified in a timely manner
- incorrect recognition of borrowings and cash and cash equivalents
- land assets not held at their fair value with revaluation recognised through revaluation reserve
- not correctly accounting for their share of investment in associate
- overstatement of employee benefits and misclassification between the current and non-current portion of long service leave provisions.

Also disappointing was the number of entities submitting many versions of their financial statements to us during the audit process. This results in significant additional work for both the entity and the auditor, and delays the finalisation of the audit. For example, one entity submitted 21 versions of its financial statements.

To ensure timely and accurate financial reports it is important that management in each reporting entity keeps proper accounts and records. Management should undertake appropriate oversight reviews of systems and processes throughout the financial year and after year end to improve the quality of their financial reporting.

To assist public sector entities to assess their financial management and reporting practices, our Office tabled the *Western Australian Public Sector Financial Statements – Better Practice Guide*. This practical guide and toolkit set out better practice principles which, when applied, support a strong governance framework and an efficient and effective financial statement preparation process. While the guide is not prescriptive or obligatory, it should assist entities to implement better practices, processes and procedures, and achieve more efficient and timely financial reporting for their entity.

Each year when we table our annual audit results report of State government entities, we assess them on their financial reporting and financial controls. We then recognise those State entities that achieve good practice by assessing the number and significance of control

weaknesses, the quality of their financial statements, audit readiness, management resolution of accounting standards and the availability of key staff during the audit process.

In 2021-22, we will examine the local government sector and recognise the top best practice entities in our annual audit results report. On page 10 we have outlined our assessment criteria. We hope that reporting top achieving entities from across the sector will increase the effectiveness and efficiency of the financial statement preparation process and contribute to improving the quality of financial reports submitted for audit.

Recommendation

1. We encourage entities to make use of our *WA Public Sector Financial Statements – Better Practice Guide* to improve their financial management and reporting practices, processes and procedures.

Summary of audit opinions

For the financial year ending 30 June 2021 we issued clear auditor's reports for 130 entities by 30 June 2022. Two audit opinions were modified (qualified), while we included emphasis of matter paragraphs in the audit reports of 24 entities.

The auditor's report includes:

- the audit opinion on the annual financial report
- any significant non-compliance in relation to the financial report or other financial management practices
- any material matters that indicate significant adverse trends in the financial position of the entity
- other matters the auditors deem necessary to highlight.

Under the LG Act, an entity's chief executive officer (CEO) is required to publish its annual report, including the audited financial report and the auditor's report, on the entity's website within 14 days of the annual report being accepted by the entity's council. Appendix 1 outlines the date we issued each entity's 2020-21 auditor's report.

We also finalised the 2019-20 auditor's report for two entities.

Two disclaimers of opinion for 2019-20

On 16 June 2021, we tabled the results of 117 entities' 2019-20 financial audits in Parliament. On 24 November 2021, we reported a further 13 entities' results in our State government entities audit report. At that time, results remained outstanding for the Shires of Wiluna and Yalgoo. We were unable to express an opinion on their financial audit reports and have now issued them a disclaimer of opinion.

For both entities, we were unable to obtain sufficient appropriate audit evidence on the books and records of the Shires. This was due to numerous significant deficiencies in the Shires' internal controls and in some cases, records not being adequately maintained. See Appendix 2 for the full details of the disclaimers.

The absence of sufficient appropriate evidence is a significant impediment for the auditor and a serious matter for both the auditor and those who rely on the auditor's opinion. If an auditor is unable to obtain the required evidence, they have few options. One option is to issue a disclaimer of opinion.

Such an opinion is only issued after we have exhausted our efforts to achieve the desired audit objectives. It is the first time this Office has issued such an opinion for a local government entity since becoming responsible for auditing the sector in 2017. It is also the first issued by our Office on a financial report for any WA government entity in 25 years.

A disclaimer of opinion on financial statements is a serious matter as we were unable to provide assurance over financial accountability. This can lead to a lack of confidence in the appropriate use of public monies.

Given the nature and timing of these disclaimers of opinion it is, regrettably, our expectation that issues requiring these disclaimed audit opinions may continue into 2021 and 2022 in some manner. However, we are aware that both entities have been working to address these concerns since the matters were first raised.

Response from Shire of Yalgoo

The Shire acknowledges the effort of the OAG in undertaking the 2019-2020 audit. We also confirm that we recognise the seriousness of the issues raised by the audit and give our assurance that a plan of action has already been implemented. We continue to do work under that plan. The Shire would also like to identify a number of factors which influenced the audit result, including:

- resourcing constraints
- changes of CEO
- communication between Shire and audit team
- timing of release of audit report.

We are conscious that the existence of these factors does not amount to an excuse for the deficiencies identified. On the other hand, we hope their existence will go some way to helping explain how those factors, rather than a culture of disregard for the need to ensure proper controls and compliance, contributed to the audit result.

17 June 2022

Two qualified audit opinions for 2020-21

We issue a qualified opinion in our auditor's report on an annual financial report if we consider it is necessary to alert readers to material inaccuracies or limitations in the financial report that could mislead readers.

In 2020-21, two entities received a qualified audit opinion. This is an improvement from four qualifications issued in 2019-20 and six in 2018-19.

The Shires of Goomalling and Sandstone received qualified opinions because their infrastructure assets had not been valued with sufficient regularity and therefore, we were unable to determine if they were fairly stated. For the full details of the qualified opinions see Appendix 3.

Audits in progress

The 16 audits still being finalised may result in modified opinions. Generally, audits in progress relate to:

- entities having more significant or complex issues to be resolved from a financial reporting and auditing perspective
- entities not having the in-house expertise needed to manage their financial reporting.

While some entities collaborate and seek help to overcome these issues, this is often informal and ad-hoc.

Twenty-four entities received emphasis of matter paragraphs

Under Australian Auditing Standards, if a matter is appropriately presented or disclosed in the financial report, but in our judgement is of such importance that it should be drawn to the

attention of readers, we may include an emphasis of matter (EoM) paragraph in our auditor's report.

In 2020-21, 25 EoM paragraphs have been included to bring to the reader's attention to:

- restatements of comparative figures or balances (11 entities)
- restatements and guarantee payments (four entities)
- changes to the basis of accounting used by the entity (six entities)
- the recording of a joint venture (two entities)
- a contingent liability (one entity)
- an event occurring after the end of the reporting period (one entity).

A full description of these matters is at Appendix 4.

In previous years, we included an EoM in all entities' auditor's reports to draw attention to their previous recognition of some categories of land, including land under roads, at zero cost.

Seventy-five entities had 193 material matters of non-compliance with legislation

We reported 193 matters of non-compliance to 75 entities. Under Regulation 10(3)(b) of the Local Government (Audit) Regulations 1996 (LG Audit Regulations), we are required to report any matters indicating that an entity is non-compliant with:

- part 6 of the LG Act
- FM Regulations
- applicable financial controls in any other written law.

The matters may relate to the financial report or to other financial management matters.

The most commonly reported matters related to:

- financial ratios not being reported (28 entities)
- a lack of evidence that enough quotations were obtained to test the market or documentation to explain why other quotes were not sought (22 entities)
- no evidence of independent review and approval of journal postings to the financial ledger (13 entities)
- a financial management review was not completed every three years as required (13 entities)
- changes made to the supplier master files were not independently reviewed and approved (12 entities)
- bank reconciliation processes were incomplete (12 entities).

Other matters included procurement without purchase orders, incomplete monthly reconciliations of fixed assets, payroll and employment non-compliance, and purchase orders raised, approved and paid by the same person. For the convenience of Parliament and the public, we have summarised the noteworthy matters in more detail at Appendix 5.

In determining which matters to examine through audit procedures (on a risk-based sample and rotational basis) and report, we apply the principles of materiality, as required by Auditing Standard ASA 320 *Materiality in Planning and Performing an Audit*. Factors that we consider include the extent and frequency of the non-compliance, and its effect or potential effect.

We also consider Regulation 5(1) of the FM Regulations to be particularly important because failure to effectively apply those requirements can result in significant financial loss, inefficiency, financial misreporting or fraud.

If we find matters of non-compliance at an entity, we will report this in the auditor's report which becomes part of their annual report published on their website. There was no discernible trend regarding the type or size of entity to which these findings relate.

Adverse trends in the financial position of 109 entities

We conducted a high-level assessment of whether the seven financial ratios reported in each entity's financial report achieved the standards set by the DLGSC. This year, we reported that 156 ratios at 109 entities indicated adverse trends of which the asset sustainability and the operating surplus ratios were the most commonly reported as adverse. Last year, for the 2019-20 audits, the comparative figures were 139 ratios with adverse trends at 89 entities. Entities report their ratios for the current year and the preceding three years. Our trend analysis is therefore limited to these four years.

We are required by Regulation 10(3)(a) of the LG Audit Regulations to report 'any material matters that in the opinion of the auditor indicate significant adverse trends in the financial position or the financial management practices of the local government'. When determining if a trend was significant and adverse, in some instances we allowed for a ratio to be slightly lower than the DLGSC standard. We allowed this in recognition that failing to meet some standards is more significant and representative of an entity's financial position than failing to meet others.

Our financial audit assessments of the ratios are conducted objectively on the audited figures from the financial report on a comparable and consistent basis. Our assessments do not consider other aspects of the entity's finances or the inter-relationships between the ratios. These considerations are outside the scope of the legislative audit requirement of Regulation 10(3)(a) and more relevant to a performance audit into adverse trends.

We issued 275 audit certifications

In addition to the auditor's reports on annual financial statements, we also conduct audit work to certify other financial information produced by entities. These audit certifications enable entities to meet the conditions of State or Commonwealth funding or specific grant requirements or legislation (acquittals). Our audit certification of these statements may be required to enable entities to receive ongoing funding under existing agreements or to apply for new funding.

For the 2020-21 audit cycle we are responsible for conducting 139 certifications for the Local Roads and Community Infrastructure Program (LRCI Program). The \$3 billion Commonwealth-funded program supports entities to deliver priority local road and community infrastructure projects across Australia.

Under the LRCI Program, entities who are eligible for funding must provide the Commonwealth Department of Infrastructure, Transport, Regional Development, Communications and the Arts with an audited 2020-21 annual report by 31 October 2021. This must be audited by an appropriate auditor.

As defined by the *National Land Transport Act 2014*, our Office is the appropriate auditor given entities' accounts are required by law to be audited by the Auditor General of a State.

Appendix 6 lists the 275 certifications we have issued for 2020-21 and the date of issue including:

- 11 claims by administrative authorities for pensioner deferments under the *Rates and Charges (Rebates and Deferments) Act 1992*
- 136 statements acquitting Roads to Recovery funding under the *National Land Transport Act 2014*
- 125 statements acquitting the LRCI Program funding (14 certifications outstanding)
- three other certifications for projects by entities.

Control weaknesses

Management controls

We report to entity CEOs on all control weaknesses relating to expenditure, revenue, financial management, asset management and human resources. Control weaknesses that represent matters of material non-compliance form part of the overall auditor’s report that we provide under section 7.12AD of the LG Act to the mayor, president or chairperson, the CEO and the Minister for Local Government.

Our management letters provide a rating for each matter reported. We rate matters according to their potential impact and base our ratings on the audit team’s assessment of risks and concerns about the probability and/or consequence of adverse outcomes if action is not taken. We consider the:

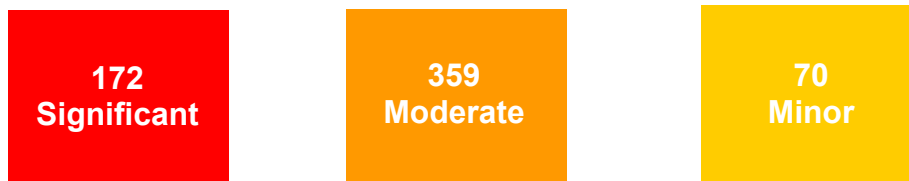
- quantitative impact – for example, financial loss from error or fraud
- qualitative impact – for example, inefficiency, non-compliance, poor service to the public or loss of public confidence.

Risk category	Audit impact
Significant	Finding is potentially a significant risk if not 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.
Moderate	Finding is of sufficient concern to warrant action being taken by the entity as soon as practicable.
Minor	Finding is not of primary concern, but still warrants action being taken.

Source: OAG

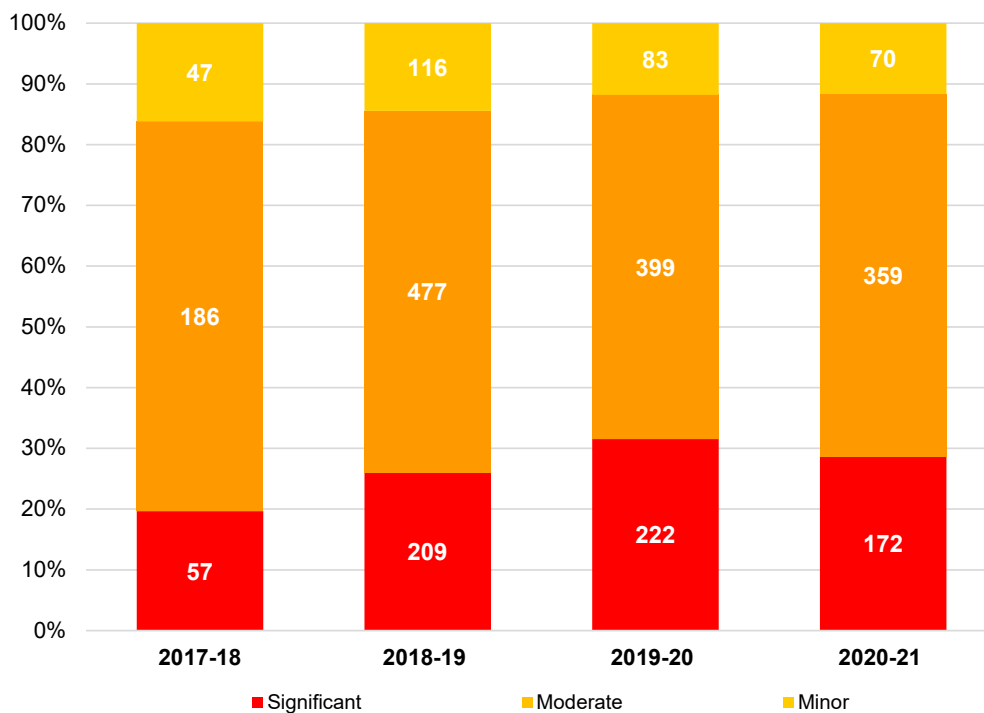
Table 2: Risk categories for matters reported to management

During 2020-21, we alerted 126 entities to control weaknesses that needed their attention. In total we reported 601 control weaknesses across the three risk categories as shown in Figure 1. This is a decrease compared to the figures from 2019-20 where we reported 704 control weakness of which 222 were significant, 399 moderate and 83 were minor findings.



Source: OAG

Figure 1: Number of financial and management control findings by risk category for 2020-21



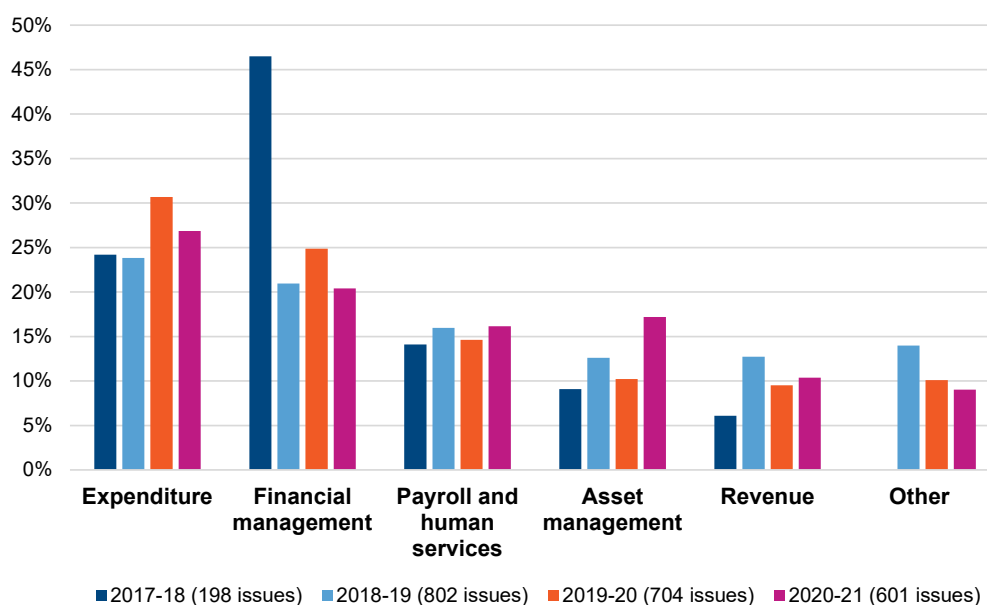
Source: OAG

Figure 2: Proportion of control weaknesses reported to management in each risk category and comparative ratings of the control weaknesses

Figure 2 shows the number of weaknesses in each risk category for the differing number of entities we audited during our first four years of local government auditing and the comparative proportion of weaknesses in each risk category. The chart shows that the number of control weaknesses across all ratings has decreased for 2020-21, noting that each year’s figures represent findings across an increasing population of audited entities during the transition period.

However, we found that 95 control weakness (15.8%) at 39 entities were unresolved from the prior year. This proportion compares with 2019-20 where 15% of issues were unresolved from the prior year. It is important that these issues are addressed promptly and requires entities to improve policies, practices and procedures to maintain or enhance the integrity of financial reporting.

The 601 control weakness identified in 2020-21 are presented in their different financial management control categories in Figure 3. This figure also shows that expenditure and financial management controls continue to represent the highest proportion of weaknesses across the financial control environment. However, it was pleasing to see that the control weaknesses relating to expenditure, financial management, and payroll and human resources have decreased for 2020-21. This is a positive trend. An increase in audit findings related to asset management suggests greater focus may also be required by entities on the controls around this aspect of financial management.



Source: OAG

Note: In 2017-19, no control weaknesses were reported in the Other category.

Figure 3: Financial and management control weaknesses reported to entities

Following are examples of control weaknesses identified in the major categories of audit findings.

Expenditure

We reported that good procurement procedures, such as obtaining quotes and completing purchase orders to start the ordering process and accountability trail, were not routinely practiced. In summary:

- We found purchase order control weaknesses at 33 entities. Purchase orders were often raised after the goods had been supplied or after the supplier’s invoice had been received. The lack of adequate controls over purchase ordering increases the risk of inappropriate purchases or the entity being committed to pay for purchases made by officers who do not have authority or who have exceeded their delegated purchase limits.
- At 22 entities we continued to find instances where quotes were not obtained as required by the entities’ policy guidelines. There were also instances where evidence of quotes was not kept. This increases the risk of favouring specific suppliers and/or not obtaining value for money.
- At 15 entities we reported that changes were made to the supplier master file without appropriate evidence of authorisation or there was no independent review to confirm checking for related party interests, authorisation, completeness and accuracy. These review procedures are essential as technology has increased the risk of fraud.
- We identified credit card control weaknesses at 14 entities. These included instances such as:

- transactions not listed separately in the payments submitted to council each month
- certain staff allocated a credit card who had not signed a credit card holder agreement
- no evidence of independent review for staff credit card monthly expenditure
- receipts not available for certain credit card transactions.
- In some entities there was not adequate separation of tasks between ordering and receiving goods. Without this segregation, the entity needs other controls to ensure that all payments for goods are reviewed and authorised by an independent officer.

Financial management

The accounting procedures and practices of the financial management team should include appropriate controls for preparing the entity's financial report and mandatory annual reporting requirements.

- At 27 entities we found that bank reconciliations were either not routinely prepared on a monthly basis or were not reviewed by a second officer. The bank reconciliation is a key control. If not performed regularly and independently reviewed, there is a risk of erroneous or unusual (including fraudulent) reconciling items not being detected and investigated in a timely manner.
- At 17 entities we found instances where journal entries were made without supporting documentation or were not reviewed by an independent officer. These can represent significant adjustments to previously approved accounting transactions. Unauthorised journals could result in errors in financial reports or fraud. They should therefore be clearly explained and subject to independent review.
- At 15 entities we found a lack of review of policies and procedures.
- At 11 entities we found that access to the financial management, payroll and human resources systems was not restricted to appropriate staff. In some instances, we considered more staff than necessary had passwords to access key systems. Access privileges need to be monitored on a regular basis by a senior staff member.

Payroll and human resources

Payroll and human resource management are essential elements of any employer's business. During our interim and final audits of entities we reported:

- Across 20 entities we found some employees were not taking their annual and long service leave entitlements and therefore accumulating excessive leave balances. Entities should have a leave management plan to ensure suitable staff can undertake the roles of key staff while they are on leave and to continue to deliver the entity's required services. Infrequent taking of leave and associated rotation of staff roles increase the likelihood of fraud remaining undetected.
- At 12 entities we found commencement and termination processes were not completed promptly to ensure timely and accurate processing and payment of staff. Evidence needs to be retained of all employment contracts, which should be signed by both parties on execution.
- At 12 entities we found monthly payroll reconciliations were not prepared in a timely manner and independently reviewed, increasing the risk of errors and/or potential fraud remaining undetected and misstated financial statements.

- At 11 entities we found instances where changes made to employee master files were either not supported by appropriate authorisation from the employee or not independently reviewed for accuracy and completeness. This is important to reduce the risk of payroll errors or fraud.

Asset management

We identified several weaknesses in the controls over assets. These included:

- a lack of evidence of review of fixed asset reconciliations at 14 entities
- asset management plans not completed or sufficiently updated at eight entities. This may impact the strategic planning process and is likely to result in misstatement of the asset renewal funding ratio in the financial report
- no asset stocktake policy or procedures in place at seven entities. The absence of a periodic asset stocktake means that discrepancies between the accounting and physical records will not be detected and corrected on a timely basis. This could result in failure to detect theft or loss and/or a misstatement of asset balances in the annual financial report
- a lack of comprehensive asset management procedures to manage non-current assets at six entities. Good policies and procedures provide essential guidance for staff to manage an entity's assets in accordance with management's expectations. Lack of formal and comprehensive policies and procedures that are readily available to staff increases the risk of mismanagement and recording of assets.

Other asset issues we found included:

- the entity not performing an assessment to determine the correct classification of vested improvements on vested land required to be separately classified as right-of-use assets
- asset revaluations not completed in a timely manner
- no documented inventory control policy and procedure for employees to follow to ensure that inventory is physically safeguarded and all movements are recorded accurately and completely in the accounting records
- incorrect application of the useful life of assets in depreciation calculations which could result in an over/understatement of the depreciation and hence of the carrying value of the assets in the financial statements.

Revenue

Good controls over revenue help to ensure that all monies due to the entity are accurately charged, collected and reported in the financial statements. During our interim and final audits, we reported:

- charges being raised prior to a completed review of the rates billing verification register
- fees were not correctly recorded in the financial system and customers were charged the incorrect fee
- no register of infringements issued by the entity
- interim rate notices had not been issued throughout the year by the entity
- rateable values reconciliation not completed

- a lack of a formal process to assess the revenue recognition criteria for new grant funding received
 - revenue not recognised in accordance with AASB 15 or AASB 1058. As application of these standards may result in delayed income recognition, the entity's revenue may be overstated for the 2020-21 financial year.
-

Recommendation

2. Local government entities should ensure they maintain the integrity of their financial control environment by:
 - a. periodically reviewing and updating all financial, asset, human resources, governance, information systems and other management policies and procedures and communicating these to staff
 - b. conducting ongoing reviews and improvement of internal control systems in response to regular risk assessments
 - c. regularly monitoring compliance with relevant legislation
 - d. promptly addressing control weaknesses brought to their attention by our audits, and other audit and review mechanisms
 - e. maintain currency with new and revised accounting standards for their impact on financial operations in order to prepare a compliant financial report at year end.

Information system controls

In 2020-21, we reported 358 information system control weaknesses to 45 entities, with 10% (37) of these rated as significant and 71% (254) as moderate. Last year we reported 328 control weaknesses to 50 entities. As these weaknesses could significantly compromise the confidentiality, integrity and availability of information systems, entities should act promptly to resolve them.

Entities rely on information systems to prepare their financial statements and to deliver a wide range of services to their communities. It is important that entities implement appropriate controls to maintain reliable, secure and resilient information systems.

Audits of general computer controls help entities measure and improve the effectiveness and reliability of services and financial reporting. These audits are performed as an integral part of, and inform, our financial audit program

Our capability assessments at 12 of the 45 entities show that none met our expectations across all six control categories and 68% of the audit results were below our minimum benchmark. Information and cyber security remain significant risks again this year and need urgent attention. Compared to 2019-20, there have been some improvements in change control but very little progress in management of information technology (IT) risks, physical security and IT operations. Entities need to improve in all six control categories.

Of the weaknesses identified in 2020-21:

- 47% related to information security issues. These included system and network vulnerabilities, and unauthorised and inappropriate access
- 28% related to IT operations issues. In particular, there were issues in inadequate monitoring and logging of user activity, poor handling of information and lack of review of user access privileges
- 13% related to business continuity. For example, disaster recovery and business continuity plans were lacking or out-of-date
- 12% related to inappropriate IT risk management, poor environmental controls for the server room and a lack of change management controls.

The information provided above is included in our *Information Systems Audit Report 2022 – Local Government Entities*, tabled on 28 June 2022. Further details of the information systems audit work and case studies are included in that report.

Issues impacting entity reporting

Rehabilitation of landfill sites

Issue

Many entities have landfill sites which they manage. Depending on the size and scale of these sites, there are different requirements to rehabilitate them. Where entities have an obligation to remediate the landfill site, they should include the rehabilitation costs as a provision in their financial report. The absence of a rehabilitation plan and cost estimate does not remove the need to record a provision.

From the time it is evident that recognising a liability is required, to actually reporting one, a process of planning is needed, and this can take a while. In the meantime, readers should be alerted to the fact that a liability will be created by the entity showing a contingent liability in their financial reports. This is shown in the example below.

What we found

We've found that some entities are not including these provisions for rehabilitation and others that are, are accounting for them differently. There is a possible role for the DLGSC to provide guidance in this area to ensure entities are correctly accounting for rehabilitation provisions.

Example: City of Kalgoorlie-Boulder

The City has operated the Yarri Road Refuse Facility in east Kalgoorlie since 1993. The site operates under a Class II landfill license under Part V of the *Environmental Protection Act 1986* which requires licensing.

The City has never previously recognised a provision for landfill rehabilitation. It has disclosed a contingent liability for at least the three previous annual financial reports to fully restore the site at the end of its useful life. The City was also undertaking work to establish the scope and estimate the cost of the restoration, which was unable to be reliably estimated in previous financial reports.

During the 2020-21 period, the City engaged a third-party expert to prepare a closure and post-closure management plan and provide a comprehensive estimation of the future costs for the site closure, capping, restoration and monitoring activities. The plan was finalised in March 2021 and a landfill rehabilitation provision of \$28.8 million was recognised.



Source: OAG

Figure 4: Broome landfill

Recommendation

3. The Department of Local Government, Sport and Cultural Industries should provide guidance to assist entities with understanding the requirements of and interpreting the AASB accounting requirements to ensure greater accounting consistency across the sector, including recognising provisions for the rehabilitation of landfills and other contaminated sites.

Valuation of assets

Issue

As reported in previous years, we have concerns about inconsistencies in the valuation of property and infrastructure in the local government sector, including the variety of valuation methods used, especially for land assets with restricted use.

Valuation concerns arise from entities engaging different valuers who use different methods or interpret some principles of the Australian Accounting Standards differently. Consequently, entities can see significant valuation swings when they change their valuer, depending on which assumptions the valuer uses. Most entities revalued their restricted land assets in 2017 or 2018 in accordance with the FM Regulations. Their next three to five yearly valuations are due at the latest by 2022 or 2023.

As mentioned last year, the AASB and the International Public Sector Accounting Standards Board have projects underway relating to fair value of public assets. Our Office will work with other audit offices to prepare a submission to these fair value projects and with the DLGSC on the audit impacts of any changes.

Even though a formal valuation is not required to be undertaken every year, the requirement for such assets to be at fair value remains. Thus, each entity needs to do enough, at a minimum, to be able to conclude that the carrying value at the reporting period approximates its fair value. This would entail, amongst other things, condition assessments, assessing recent pricing movements in materials and labour, and other relevant material factors.

What we found

A few examples of entities experiencing some valuation issues were:

- City of Albany – the City has no formal process for assessing the valuation of infrastructure assets, land and buildings in financial years between the formal valuation assessments required by the FM Regulations. Without this, an asset may not be correctly recorded at fair value in accordance with AASB 116 and AASB 13. The City was notified of the finding during an interim audit and completed an assessment as part of its end of financial year procedures.
- City of Subiaco – the City's investment property increased by \$12.3 million (11%) compared to the prior year due to a revaluation to fair value at 30 June 2021 based on an independent valuation of \$125 million, which resulted in a net gain of \$29 million. The City also reported an increase to Revaluation Surplus of \$35.8 million (28%) compared to the prior year.
- Town of Cottesloe – during 2020-21, an independent valuation of land and buildings resulted in a decrease in fair value of \$20.5 million compared to the prior year. This related to an interest the Town has in the Wearne Hostel (refer below).

- Four entities hold an equal share in the Wearne Hostel site at 1 Gibney Street, Cottesloe but value it differently. We found one valuation almost double that of the other. The Towns of Claremont and Mosman Park have valued their respective interests separately without restrictions, while the Shire of Peppermint Grove and Town of Cottesloe have valued with restrictions (i.e. title showing zoning for use only as an aged care facility), resulting in a much lower valuation. We acknowledged the inconsistency in financial reporting for the same asset but accepted both valuations (restricted and unrestricted) as they are currently permissible under the relevant accounting standard and DLGSC financial reporting framework.

Developer contributions – Accounting for cash in lieu of public open space

Issue

When subdividing residential land in WA, a minimum of 10% of the gross subdivisible area must be given up free of cost by the landowner for public open space. The landowner can make a cash payment to an entity in lieu of all or part of the public open space contribution, which must be agreed by the entity and approved by the Western Australian Planning Commission.

Amendments to section 154 of the *Planning and Development Act 2005* (PD Act) changed the accounting treatment for cash in lieu of public open space contributions received on or after 12 September 2020. Entities receiving any cash in lieu funds should now place them in a reserve account for each subdivision within the municipal account, in accordance with section 6.11 of the LG Act.

The account should clearly set out the purpose for which the money is held, the landholding from which it was obtained and the date on which it was paid to the entity. Section 154(3) of the PD Act also requires interest earned on any invested funds to be applied to the respective reserve account.

The DLGSC provided guidance to entities on the accounting treatment for cash in lieu received on or after 12 September 2020, from 10 April 2006 until 11 September 2020, and prior to 10 April 2006. One entity sought its own legal advice.



Source: bumphotographer/shutterstock.com

Figure 5: Park and playground in a suburban area of Perth

What we found

While some entities were not prepared, the majority of affected entities accounted for the funds appropriately and complied with revised legislative requirements.

Some entities had differing treatments, for example:

- We noted that money paid to the City of Albany in lieu of open space, post 12 September 2020 and amounting to \$30,000, was not placed in a reserve account in accordance with section 6.11 of the LG Act. On being notified of the finding during the interim audit, the City rectified this as part of their annual procedures, had a newly created public open space reserve account endorsed by Council and correctly reported the received funds in the annual financial statements for the year ended 30 June 2021.
- The City of Cockburn, on obtaining legal advice, chose to adopt a different accounting treatment than recommended by the DLGSC. It accounted for all cash in lieu of public open space in the municipal fund, rather than some in trust and some in the municipal fund.
- We found the accounting for cash in lieu by the City of Greater Geraldton is classified in accordance with the PD Act, with an exception that funds amounting to \$378,000 should have been classified as trust rather than in reserves, as it was received between 10 April 2006 and 11 September 2020. We accepted this as reasonable and agreed with management on the classification of the funds.

Implementation of Service Concession Grantors Standard AASB 1059

Issue

Entities were required to apply a new standard, AASB 1059 *Service Concession Arrangements: Grantors*, for years beginning on or after 1 January 2020 (the 2020-21 reporting year). This standard is applicable to entities (grantors) that enter service concession arrangements with generally private sector operators.

It requires grantors to recognise a service concession asset and, where applicable, a service concession liability on the balance sheet. Alternatively, a service concession asset may result from the reclassification of an existing item of property, plant and equipment.

An arrangement within the scope of this standard typically involves an operator constructing the assets used to provide a public service or upgrading the assets (for example, by increasing their capacity) and operating and maintaining the assets for a specified period. Such arrangements are often referred to as public-private partnerships.

An example of a major service concession arrangement for WA local government is the Resource Recovery and Facility Agreement involving the Mindarie Regional Council, a regional entity, and its constituent member entities - the Cities of Perth, Stirling, Joondalup, Wanneroo and Vincent, and the Towns of Victoria Park and Cambridge.

Under this agreement the operator constructed and has the responsibility to manage the facility for the purpose of waste processing activities on behalf of the Mindarie Regional Council. The agreement was entered into for a 20-year term ending June 2030. On termination of the agreement, the Mindarie Regional Council would assume all rights and responsibilities in relation to the assets and liabilities of the Service Concession Arrangement.

What we found

For most entities there was no material impact to the financial statements in 2020-21.

Other changes to accounting standards

What we found

As we reported in November 2021⁵, the reporting of revenue and income by not-for-profit entities under AASB 15 and AASB 1058, which were applied from 1 July 2019, has brought challenges in interpretation and implementation. It is expected that the AASB will propose further guidance and examples in 2022 that have the potential to change current accounting practice.

⁵ Office of the Auditor General, [Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities](#), OAG, Perth, 2021, p 43.

Impact of emergencies

COVID-19

We have continued to note the impact of COVID-19 responses on entities' financial reporting processes and control environments. Part of our 2020-21 audits considered the impact faced by entities, given State and international border restrictions were in place during the financial year and in February, April and May 2021 the WA Government announced lockdowns and other restrictions in response to managing COVID-19 community transmission. Some of the impacts are summarised below.

Disruption of services and reduced revenue

Entities were faced with venue closures and restrictions for public and private gatherings resulting in event cancellations and reduced capacity. A few examples identified during our audits are listed below where entities experienced an impact to the community and disruption of services:

- City of Greater Geraldton – reported that Recreation and Culture income was down from \$4.2 million in the prior year to \$1.6 million in 2020-21 (62%). This decrease is mainly due to the recreation and culture sector being heavily impacted by COVID-19 restrictions including the stand down of theatre and events staff. The Queens Park Theatre was completely closed for the nine months to March 2021 with partial reopening from April to June 2021. All events and cultural projects at the City were either scaled back or not held due to State mandated restrictions.
- City of Melville – the City reported a 10% decrease in rates revenue for 2020-21 compared to the prior year. Rates concessions (approved by the Council in April 2020) applied in the 2020-21 budget under the COVID-19 Stimulus package amounted to approximately \$10 million. The City also reported a 56% decrease in interest earnings from \$4.4 million in the prior year to \$1.9 million in 2020-21. As part of section 6.45 of the LG Act modified under the Local Government (COVID-19 Response) Order 2020 to cushion ratepayers from the adverse economic effects of COVID-19, the City reduced interest rates to 2% on:
 - unpaid rates subject to an instalment program (previously 4%)
 - all unpaid rates and services (previously 8%)
 - unpaid underground power and streetscape charges (previously 4%).

This also led to a decrease in rates receivable balances at year end.

- The City of Rockingham – committed to a rate freeze for 2020-21 due to the COVID-19 pandemic. In addition, the City provided a concession totalling \$846,773. The concession was to ensure that residential properties were not charged more rates than they would have paid in 2019-20 due to the statutory Gross Rental Value revaluation the City was required to apply. The City also reduced interest rate charges on unpaid rates and other service charges and therefore reported a \$2.2 million (67%) decrease in interest earnings compared to the prior year. Payments by residents however have continued to be repaid in 2021 with a resulting effect of lower receivable balances compared to the prior year.
- City of Stirling – as part of the City's COVID-19 response in 2020-21, the Council committed to a one-off concession to ensure no ratepayer was asked to pay more than the previous year. The City also introduced rates smoothing in addition to its one, two

and four instalment options. In accordance with the Local Government (COVID-19 Response) Order 2020, the City did not charge

- interest where an owner selected to pay rates and service charges through an instalment option
- overdue interest to ratepayers with overdue rates and service charges.
- Shire of Harvey – reported a reduction in interest earnings from \$1.3 million in the prior year to \$395,000 in 2020-21 (69%) mostly due to the decrease in interest rates paired with a decrease in interest earnings from rates revenue due to rate relief from COVID-19.
- Shire of Ngaanyatjaraku – statutory environmental health functions such as food inspections were delayed as they were not deemed to be an essential service by the WA Police Force and G2G passes were not approved for the visiting environmental health officer. Indoor sport and recreation activities were cancelled and program changes were made to enable limited activities to provide food and essential services in compliance with COVID-19 directions.

Entities' expenses for directly managing the impact of COVID-19

Differentiating between COVID-19 specific expenditure and normal expenditure was difficult as entities generally did not separately account for these expenses. In general, entities did not report incurring any significant expenditure as potential extra expenses were offset by savings elsewhere. Some interesting examples are noted below:

- Shire of Broome – the Shire's current three year COVID-19 recovery plan focuses on significant infrastructure projects. The State and Commonwealth Governments have co-invested in most of these projects. The intent of the projects is to reinvigorate the region and stimulate the local economy (e.g. jobs and tourism) which will assist in COVID-19 recovery.
- Shire of Denmark – the Shire experienced challenges in securing contractors and equipment from interstate and intrastate due to COVID-19 restrictions. Cost of contractors, materials and supplies has risen on average 20% over the past 12 months. Due to significant increases in available State and Commonwealth funding, it is increasingly difficult to secure available contractors to complete works within funding condition timeframes. The impact of COVID-19 has fast-tracked the Shire to implement more services and application processes online for the community to access.
- Shire of Dowerin – while the financial impact of COVID-19 on the Shire was minimal throughout 2020-21, additional resources were allocated including:
 - staff resources to keep up-to-date with relevant information and mandates
 - preparing and implementing the Shire's COVID-19 plan and working-from-home processes
 - increased community communication and engagement
 - additional cleaning.

The Shire had also experienced delays in completion of road construction and building projects due to contractors not being available and an increased cost of materials, freight and contractors.

- Shire of Gnowangerup – the main impact for the Shire includes significantly reduced availability of contractors, particularly building-related trades, and reduced availability of

vehicles. This has impacted the Shire's ability to complete projects within timeframes and budgets. Some capital expenditure items in the current year budget will carry over to the new financial year as a result.

Stimulus or initiatives administered by entities

Below are some examples where entities played a role in distributing funds and providing relief to their communities in 2020-21:

- City of Gosnells – the City reported \$1.4 million in COVID-19 concessions for ratepayers and relief for lessees.
- City of Greater Geraldton – the City offered rent relief to some tenants who were badly affected by the pandemic. The rent relief was in line with the *Commercial Tenancies (COVID-19 Response) Act 2020* and was available to tenants that had experienced a reduction of revenue of at least 30% over the previous year. The relief was in two parts: a portion of the rent was to be waived and another portion was to be deferred.
- City of Kalamunda – a COVID-19 Crisis Relief Fund reserve was established by the City at the beginning of the financial year of \$1 million to provide innovation grants of up to \$5,000 and \$1,000 rate relief to each eligible ratepayer. However, only \$216,000 was paid out during the year to 30 June 2021. The balance of the fund was returned to the City's bank account and the Crisis Relief Fund reserve was closed with the Council's approval. The City also offered a total of \$22,000 in rates exemptions under its COVID-19 financial hardship policy for the year ended 30 June 2021.
- City of Karratha – the City received a one-off contribution of \$1 million from Rio Tinto for COVID-19 recovery which was used to support the City's business and community funding packages. This included Try Local Vouchers, sporting group grants, tourism operator incentives, health fee waivers, business grants and Meet the Street funding. In addition, the City provided a number of other COVID-19 business and community support initiatives such as a freeze on rate and fee increases, deferral of rate collection, financial hardship support and lease fee relief.
- City of Subiaco – in response to the pandemic, the City resolved through its annual budget 2020-21 to provide a one-off contribution of \$2 million against total rates levied. This contribution was funded through a transfer from the Capital Investment Reserve. The \$2 million contribution to rates was applied proportionately to the number of rates levied per property, including properties paying minimum rates.
- Shire of Dalwallinu – the Shire adopted a financial hardship policy during 2019-20 to assist the community members who may have been affected by the COVID-19 pandemic. This policy was amended during 2020-21 to also include other unexpected items that may result in payment difficulties.
- Shire of Dandaragan – the Shire implemented a range of measures to respond to the challenges of COVID-19 including removing or heavily discounting interest charges on rates and debts, deferring community group loans and providing \$5,000 cash grants to community groups to enhance their facilities. A significant increase in infrastructure investment was undertaken targeting civil works that could employ the local workforce, in particular deckhands, who were impacted by disruption to the crayfishing industry. A COVID-19 community building program was established to support those at high risk including seniors, people with a disability or underlying health issue, people from culturally and linguistically diverse backgrounds, and indigenous people. The Shire also developed a COVID-19 webpage providing information and tools for its community such as the COVID-Readiness Household Plan.

Future potential effect of COVID-19

As responses to COVID-19 continue to impact well beyond this reporting period and constrain the functions and responsibilities of entity operations, the risk increases that other critical areas may not receive the focus or priority they deserve. We encourage staff and management to be mindful of gaps where more visible financial and operational controls may cease to operate effectively, including in altered work arrangements such as staff working from home.

Cyclone Seroja

On 11 April 2021, Cyclone Seroja intensified into a category 3 tropical cyclone and crossed the WA coast just south of Kalbarri. Impacts to Kalbarri and the nearby town of Northampton were severe, with many locations recording maximum wind gusts more than 170 km/h. Many buildings and roads sustained significant structural damage or were destroyed. An emergency situation was declared at 3.50 pm on 11 April for 45 local government areas. Services were disrupted, facilities were closed and significant damage occurred to critical infrastructure. Secondary impacts included loss of power and communications for an extended period, and a primary focus for affected communities on repair and recovery.

Examples of the financial implications arising from this emergency event in the region are as follows:

- Shire of Mingenew – at its May 2021 Ordinary Council Meeting, Council voted unanimously to waive a range of building and planning application fees to assist those impacted to rebuild, and waived some planning requirements for temporary buildings at its August 2021 Ordinary Meeting.
- Shire of Northampton – cyclone damage led to a write-down of Property, Plant and Equipment of \$1.1 million and Infrastructure of \$178,000 for the 2020-21 financial year. Additional funding of \$500,000 was received from the Local Government Insurance Scheme for operational repairs, and materials and contracts costs increased by \$1 million from \$2.3 million in the prior year to \$3.3 million in 2020-21 due to additional work required to restore the Shire's townsites.
- Shire of Chapman Valley – damages to the Shire's assets were not extensive. However, the cyclone impacted staff resources due to time taken away from core business to attend to local recovery initiatives. During the financial year the Shire restored some properties and certain work had to be carried forward to financial year 2021-22.
- City of Greater Geraldton arranged additional resources immediately following the cyclone to aid clean-up efforts. The City also spent more than \$500,000 on clearing vegetation and concentrated on rural road maintenance and removing and mulching fallen vegetation.
- Shire of Morawa experienced 202 requests for emergency welfare assistance, with 104 homes damaged and 23 primary producer properties impacted. The council spent \$141,962 in the immediate response to the cyclone with the majority being for the clearing of roads, removing fallen trees and town clean-up.

Opportunities for the DLGSC to improve the efficiency of financial reporting

Our audits have once again highlighted the need for the DLGSC to provide centralised professional support to assist entities to fulfil their financial reporting requirements. We have previously raised the need for the DLGSC to provide professional advice on preparing for changes in accounting standards and legislation. This would be both financially beneficial and time efficient for all entities. This section includes updated information on the steps the DLGSC is taking to enhance financial reporting, reduce complexity and costs, and enable improved governance. It is important to note that while some of these issues may relate to all entities, others may only be applicable to some.

Quality and timeliness

In 2019-20, and in prior reports, we reported that many entities would benefit from centralised support from the DLGSC similar to that provided to State government entities by the Department of Treasury through the Treasurer's Instructions. This would help to improve the overall quality of the sector's financial reports and also reduce the reporting burden on smaller entities. We identified the need for actions such as:

- decluttering entities' financial reports
- implementing tiered reporting for entities that differ in the size or complexity of their operations
- providing a model financial report with current sample notes
- providing technical and accounting standards support to entities through a help desk.

Further, we suggested the DLGSC's support should pursue timely regulation amendments and provide suitable guidance to assist entities to update their accounting practices. This would help ensure that their future reporting is compliant with all current accounting standards and improve the financial report framework.

While our Office produced the *Western Australian Public Sector Financial Statements – Better Practice Guide* to assist entities to implement better practices for more efficient and timely financial reporting, centralised assistance offered by the DLGSC will achieve consistency, improve financial reporting standards and could offer practical accounting assistance.

Response from the DLGSC

DLGSC has made significant progress towards addressing the recommendations via its local government model financial statements project which commenced in September 2021. DLGSC expects to fully address all recommendations by the end of financial year 2022-23. This has been largely driven by DLGSC's commitment to deliver efficiencies and better financial reporting outcomes for the local government sector. As a result, DLGSC has met and is on track to meet several critical milestones, including:

- delivery of the first tranche of decluttered financial reports for 2021-22 by 1 July 2022. The required amendments to the FM Regulations and LG Audit Regulations were gazetted on 17 June 2022
- delivery of a further second tranche of decluttered financial reports for 2022-23 by 28 April 2023
- implementing reduced financial reporting for smaller entities for the financial year 2022-23, onwards
- providing model financial statements templates with guidelines for the financial year 2022-23, onwards
- providing technical and accounting standards support from June 2022 via a dedicated email support line.

Review of financial ratios

We are required by Regulation 10(3)(a) of the LG Audit Regulations to report 'any material matters that in the opinion of the auditor indicate significant adverse trends in the financial position or the financial management practices of the local government'.

It has been our view since becoming the auditor for the sector that the annual financial report audit does not provide the opportunity for a thorough assessment of any adverse trends that may be apparent from the ratios. We have also previously supported the need for the DLGSC to develop more thorough and balanced performance assessment criteria to replace the existing reporting and audit of seven financial ratios and any adverse trends in these ratios.

In 2019-20, we also reported that the Western Australian Local Government Association (WALGA) had recommended changes to the ratios in its Local Government Financial Ratios Report provided to the WALGA State Council Meeting on 5 May 2021. The report included recommendations for prescribed ratios and other financial reporting related matters. Along with ratio changes, the group also recommended the DLGSC prepare a model set of financial statements and annual budget statements in consultation with the local government sector.

Response from the DLGSC

The DLGSC has taken on board the OAG's views and recognised the contributions of key stakeholders in respect of the financial ratios and their intended purpose and outcomes. The DLGSC's approach to financial reporting of ratios has been largely underpinned by the OAG recommendations and the need to bring local government financial reporting in line with better practice frameworks.

While the DLGSC has taken action to remove the reporting of financial ratios from the 2021-22 annual financial report, and the audit reporting of significant adverse trends and attestation of ratios, it is still committed to ensuring reliable information on local government financial and sustainability measures is available.

The DLGSC is undertaking a comprehensive review of the current financial health indicator, taking into consideration WALGA's Financial Ratios Working Group recommendations. The review will assess the appropriateness of the current financial ratios and recommend a set of financial and sustainability measures that are evidence based and fit for purpose. This will then inform the information reported via the MyCouncil website.

The Western Australian Treasury Corporation (WATC) was engaged in late March 2022 to undertake a review of the financial health indicator to identify the most appropriate ratios to underpin it. A stakeholder group consisting of WATC, the DLGSC, WALGA, LG Professionals WA and a local government finance consultant has been established to help inform the review. Targeted stakeholder engagement is to be undertaken in due course for input and feedback on the proposed ratios and methods used to underpin the new financial health indicator.

The scope prepared for WATC requests that a report and new financial health indicator product is provided to the DLGSC by 31 August 2022. The DLGSC will then review the outcomes of the report before implementing the changes for the MyCouncil website in 2023.

Reduced disclosure reporting by entities

The quantity of information that is reported in the annual financial reports of entities is onerous and exceeds that reported by most State government entities. Entities also include several disclosures that are not common practice in other Australian states. This contributes to the time and cost to prepare and audit annual financial reports.

In 2019-20, we reported that opportunities still exist to introduce a tiered reporting structure and reduce the amount of detail in entity financial reports without impacting the usefulness and completeness for users. While the FM Regulations do not provide entities as much opportunity to reduce financial report disclosures as State government entities, we continue to encourage efforts to streamline financial framework obligations, particularly for small and medium sized entities, wherever it does not impair accountability and transparency.

Response from the DLGSC

The DLGSC fully recognises the need for tiered reporting based on complexity and size of entities, while still meeting the needs of the users of financial reports. The DLGSC has developed model financial statement templates based on Salaries and Allowances Tribunal banding.

The model financial statement template for Band 1 and 2 entities significantly reduces the existing level of disclosures required to be audited. Our recommendations to the Parliamentary Select Committee into Local Government have largely guided the DLGSC in the removal of the disclosures.

The Band 3 and 4 entity model financial statement template is also streamlined and removes further disclosures without compromising the accountability and transparency of financial reporting. The DLGSC has been working closely with the OAG to ensure critical information and compliance with Accounting Standards is retained. After sector consultation, it was agreed that the model financial statements for both Band 1 and 2, and Band 3 and 4 should be introduced from the 2022-23 financial year onwards.

Local Government Regulations Amendment (Financial Management and Audit) Regulations 2022

The first component of regulatory amendments to enable the model financial statements, the *Local Government Regulations Amendment (Financial Management and Audit) Regulations 2022*, were gazetted on 17 June 2022.

Key changes which are welcomed by our Office include the removal of the requirement for an annual financial report by an entity to include:

- financial ratios
- an auditor's opinion on financial ratios, significant adverse trends and matters of non-compliance.

The changes made to the FM Regulations will reduce local government reporting requirements and the scope of audit reports and come into effect from 1 July 2022. As some 2021-21 audits are still in train, transitional provisions apply to financial reports in relation to 30 June 2021 whose audits are yet to be finalised.

Recommendation







4. The Department of Local Government, Sport and Cultural Industries should continue to work with local government stakeholders towards the introduction of model financial statements for the 2022-23 financial year.

































Appendix 1: Status and timeliness of 2020-21 audits

We completed 132 of the 148 audits for 2020-21 by 30 June 2022. All entities are listed in alphabetical order below, as well as the type of audit opinion they received, when they received it and the timeliness of providing their financial statement to us for audit.

Timeliness of financial statements does not indicate quality. Roughly half of the entities' financial statements submitted to us for audit were not of a reasonable standard and required revisions or adjustments due to errors or disclosure requirements not being met. In some cases more than a dozen versions of financial statements were submitted to our audit teams, with changes or availability of staff or information also impacting timelines. More information on issues around quality and timeliness is provided on pages 14 and 15.

Key

Type of audit opinion		Financial statement (FS) timeliness	
Clear opinion		Received by the statutory deadline of 30 September 2021	
Clear opinion with emphasis of matter		Extension to the statutory deadline was granted and met	
Qualified or a disclaimer of opinion		Extension or statutory deadline was not met	
















Entity	Type of opinion	Opinion issued	FS timeliness
Bunbury-Harvey Regional Council		14/12/2021	
City of Albany		3/12/2021	
City of Armadale		15/03/2022	
City of Bayswater	Audit in progress		
City of Belmont		17/02/2022	
City of Bunbury		7/12/2021	
City of Busselton		15/11/2021	
City of Canning		30/11/2021	
City of Cockburn		30/11/2021	
City of Fremantle	Audit in progress		
City of Gosnells		10/12/2021	
City of Greater Geraldton		9/12/2021	
City of Joondalup		14/12/2021	
City of Kalamunda		22/11/2021	
City of Kalgoorlie-Boulder		4/05/2022	
City of Karratha		8/03/2022	
City of Kwinana		9/12/2021	

Entity	Type of opinion	Opinion issued	FS timeliness
City of Mandurah		17/12/2021	
City of Melville		9/12/2021	
City of Nedlands		30/11/2021	
City of Perth		23/03/2022	
City of Rockingham		23/11/2021	
City of South Perth		19/11/2021	
City of Stirling		23/12/2021	
City of Subiaco		17/11/2021	
City of Swan		24/11/2021	
City of Vincent		15/12/2021	
City of Wanneroo		17/12/2021	
Eastern Metropolitan Regional Council		17/11/2021	
Mindarie Regional Council		14/01/2022	
Murchison Regional Vermin Council		22/11/2021	
Pilbara Regional Council		28/04/2022	
Rivers Regional Council		30/09/2021	
Shire of Ashburton	Audit in progress		
Shire of Augusta-Margaret River		6/12/2021	
Shire of Beverley		22/02/2022	
Shire of Boddington		7/04/2022	
Shire of Boyup Brook	Audit in progress		
Shire of Bridgetown-Greenbushes		23/11/2021	
Shire of Brookton		30/03/2022	
Shire of Broome		3/12/2021	
Shire of Broomehill-Tambellup	Audit in progress		
Shire of Bruce Rock		16/12/2021	
Shire of Capel		3/03/2022	
Shire of Carnamah		12/04/2022	
Shire of Carnarvon	Audit in progress		
Shire of Chapman Valley		7/12/2021	

Entity	Type of opinion	Opinion issued	FS timeliness
Shire of Chittering		18/02/2022	
Shire of Christmas Island		14/03/2022	
Shire of Cocos (Keeling) Islands		8/04/2022	
Shire of Collie		16/02/2022	
Shire of Coolgardie		17/12/2021	
Shire of Coorow		10/03/2022	
Shire of Corrigin		16/12/2021	
Shire of Cranbrook		9/12/2021	
Shire of Cuballing		22/12/2021	
Shire of Cue		6/05/2022	
Shire of Cunderdin		18/02/2022	
Shire of Dalwallinu		16/12/2021	
Shire of Dandaragan		16/12/2021	
Shire of Dardanup		8/12/2021	
Shire of Denmark		2/12/2021	
Shire of Derby-West Kimberley	Audit in progress		
Shire of Donnybrook-Balingup		23/02/2022	
Shire of Dowerin		17/02/2022	
Shire of Dumbleyung		17/03/2022	
Shire of Dundas		6/04/2022	
Shire of East Pilbara		30/03/2022	
Shire of Esperance		10/11/2021	
Shire of Exmouth		17/11/2021	
Shire of Gingin		29/06/2022	
Shire of Gnowangerup		22/12/2021	
Shire of Goomalling	Qualified	22/12/2021	
Shire of Halls Creek		18/03/2022	
Shire of Harvey		20/12/2021	
Shire of Irwin		28/03/2022	
Shire of Jerramungup		14/12/2021	
Shire of Katanning		21/12/2021	

Entity	Type of opinion	Opinion issued	FS timeliness
Shire of Kellerberrin	✓	8/12/2021	🕒
Shire of Kent	✓	15/03/2022	🕒
Shire of Kojonup	✓	17/06/2022	🕒
Shire of Kondinin	✓	21/12/2021	🕒
Shire of Koorda	✓	25/02/2022	🕒
Shire of Kulin	✓	23/02/2022	🕒
Shire of Lake Grace	✓	18/03/2022	🕒
Shire of Laverton	✓	17/02/2022	🕒
Shire of Leonora	✓	8/12/2021	🕒
Shire of Manjimup	✓	29/11/2021	🕒
Shire of Meekatharra	⚠	3/12/2021	🕒
Shire of Menzies	✓	15/12/2021	🕒
Shire of Merredin	Audit in progress		🕒
Shire of Mingenew	⚠	10/12/2021	🕒
Shire of Moora	Audit in progress		🕒
Shire of Morawa	✓	21/12/2021	🕒
Shire of Mount Magnet	✓	4/03/2022	🕒
Shire of Mount Marshall	✓	6/12/2021	🕒
Shire of Mukinbudin	✓	17/12/2021	🕒
Shire of Mundaring	✓	10/12/2021	🕒
Shire of Murchison	Audit in progress		🕒
Shire of Murray	✓	15/02/2022	🕒
Shire of Nannup	✓	18/02/2022	🕒
Shire of Narembeen	✓	15/12/2021	🕒
Shire of Narrogin	✓	22/12/2021	🕒
Shire of Ngaanyatjaraku	✓	30/11/2021	🕒
Shire of Northam	✓	7/12/2021	🕒
Shire of Northampton	✓	17/12/2021	🕒
Shire of Nungarin	✓	16/12/2021	🕒
Shire of Peppermint Grove	✓	22/12/2021	🕒
Shire of Perenjori	✓	7/04/2022	🕒

Entity	Type of opinion	Opinion issued	FS timeliness
Shire of Pingelly		17/12/2021	
Shire of Plantagenet		16/12/2021	
Shire of Quairading		17/02/2022	
Shire of Ravensthorpe	Audit in progress		
Shire of Sandstone	Qualified	31/05/2022	
Shire of Serpentine-Jarrahdale		22/12/2021	
Shire of Shark Bay		5/04/2022	
Shire of Tammin		7/12/2021	
Shire of Three Springs		22/03/2022	
Shire of Toodyay	Audit in progress		
Shire of Trayning		23/11/2021	
Shire of Upper Gascoyne		11/11/2021	
Shire of Victoria Plains		23/03/2022	
Shire of Wagin		10/11/2021	
Shire of Wandering		22/12/2021	
Shire of Waroona		22/12/2021	
Shire of West Arthur		2/03/2022	
Shire of Westonia		16/12/2021	
Shire of Wickepin		9/03/2022	
Shire of Williams		18/11/2021	
Shire of Wiluna	Audit in progress		
Shire of Wongan-Ballidu		21/12/2021	
Shire of Woodanilling	Audit in progress		
Shire of Wyalkatchem		19/11/2021	
Shire of Wyndam-East Kimberley		22/02/2022	
Shire of Yalgoo	Audit in progress		
Shire of Yilgarn		16/12/2021	
Shire of York		16/12/2021	
Southern Metropolitan Regional Council		15/12/2021	
Tamala Park Regional Council		14/10/2021	
Town of Bassendean		15/12/2021	

Entity	Type of opinion	Opinion issued	FS timeliness
Town of Cambridge	Audit in progress		
Town of Claremont		22/12/2021	
Town of Cottesloe		16/12/2021	
Town of East Fremantle		14/12/2021	
Town of Mosman Park		3/12/2021	
Town of Port Hedland		9/12/2021	
Town of Victoria Park		20/01/2022	
Western Metropolitan Regional Council		18/10/2021	

Source: OAG

Appendix 2: 2019-20 disclaimers of opinion

Entity and opinion	Opinion issued
<p>Shire of Wiluna – Disclaimer of opinion</p> <p>It has not been possible to obtain sufficient appropriate audit evidence on the books and records of the Shire. This lack of evidence arises from numerous significant deficiencies in the internal controls implemented by the Shire and, in some cases, the necessary records not being adequately maintained.</p> <p>As a result of this matter, we are unable to determine if any adjustments might have been found necessary to the elements making up the Statement of Financial Position as at 30 June 2020, Statement of Comprehensive Income by Nature or Type, Statement of Comprehensive Income by Program, Statement of Changes in Equity, Statement of Cash Flows and Rate Setting Statement for the year then ended and related notes and disclosures.</p> <p>A qualified opinion was also issued for the year ended 30 June 2019 on the completeness of bank accounts for that year because we were unable to obtain a bank confirmation from a financial institution where at least one account was held for that year.</p>	<p>22/12/2021</p>
<p>Shire of Yalgoo – Disclaimer of opinion</p> <p>We were unable to obtain sufficient appropriate audit evidence on the books and records of the Shire. This lack of evidence arises from numerous significant deficiencies in the internal controls implemented by the Shire and in some cases the necessary records not being maintained.</p> <p>As a result of this matter, we are unable to determine if any adjustments might have been found necessary to the elements making up the Statement of Financial Position as at 30 June 2020, the Statement of Comprehensive Income by Nature or Type, Statement of Comprehensive Income by Program, Statement of Changes in Equity, Statement of Cash Flows and Rate Setting Statement for the year then ended, related notes and disclosures and the Statement by the Chief Executive Officer.</p>	<p>3/03/2022</p>

Source: OAG

Appendix 3: 2020-21 qualified opinions

Entity and opinion	Opinion issued
<p>Shire of Goomalling – Qualified opinion</p> <p>The Shire of Goomalling was issued a qualified opinion as the Shire’s infrastructure assets were last valued in June 2015 for roads, drainage and footpaths and June 2016 for sewerage and other infrastructure. Because these infrastructure assets have not been revalued with sufficient regularity or in accordance with Regulation 17A(4)(b) of the FM Regulations, we were unable to determine if infrastructure assets reported in Note 9 of the annual financial report at \$43,394,718 and \$38,841,166 at 30 June 2021 and 30 June 2020 respectively are stated at fair value in the Statement of Financial Position.</p> <p>Additionally, we were unable to determine where there may be any consequential impact on the related balances, amounts and disclosures of depreciation on non-current assets, revaluation surplus in the Statement of Financial Position and Statement of Comprehensive Income and Note 19 Total Assets Classified by Function and Activity, or if any adjustments to these amounts are necessary.</p> <p>We also issued a qualified opinion for the year ended 30 June 2020 in relation to this matter.</p>	22/12/2021
<p>Shire of Sandstone – Qualified opinion</p> <p>The Shire of Sandstone was issued a qualified opinion as the Shire’s roads and footpaths infrastructure, reported at values as at 30 June 2021 of \$37,755,629 (2020: \$36,803,492) and \$71,845 (2020: \$75,711) respectively in Note 9 of the annual financial report, were last valued in June 2014. Because the assets have not been revalued with sufficient regularity or in accordance with Regulation 17A(4)(b) of the FM Regulations, we were unable to determine if infrastructure as at 30 June 2021 of \$39,718,887 (2020: \$38,820,445) in the Statement of Financial Position is fairly stated. Additionally, we were unable to determine if any adjustments are necessary to the related balances and disclosures of revaluation surplus in the Statement of Financial Position and Statement of Changes in Equity and Note 11, Other Comprehensive Income in the Statement of Comprehensive Income and Note 17 Total Assets Classified by Function and Activity, as it was impracticable to do so.</p> <p>We also issued a qualified opinion for the year ended 30 June 2020 in relation to this matter.</p>	31/05/2022

Source: OAG

Appendix 4: Emphasis of matter paragraphs included in auditor's reports

The following list describes the matters that we highlighted through EoM paragraphs in 2021 audit reports:

Entity	Description of emphasis of matter paragraphs
City of Bunbury	Recording of joint venture – The City's opinion draws attention to Note 25 to the financial statements which states that the City's equity share in the Investment in Associate is still being negotiated and therefore cannot be reliably estimated at this time. Consequently, the investment is not currently reflected in the financial statements. The opinion is not modified in respect of this matter.
City of Busselton	Restatement of comparative balances – Our EoM draws attention to the City's Note 33 to the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
City of Joondalup	Associate entity restatement and guarantee payment – Note 23 of the financial report (a) discloses the 2020 financial impact of the initial application of accounting standards AASB 1059 from the associate entity and (b) discloses a guarantee payment made by the City subsequent to the reporting date. The opinion is not modified in respect of this matter.
City of Kalgoorlie-Boulder	Restatement of comparative balances – The opinion draws attention to Note 34 to the financial report which states that the amounts reported in the previously issues 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
City of Perth	Associate entity restatement and guarantee payment – Note 32 of the financial report which (a) discloses the 2020 financial impact of the initial application of accounting standards AASB 1059 from the associated entity and (b) discloses a guarantee payment made by the City subsequent to reporting date. The opinion is not modified in respect of this matter.
City of Stirling	Associate entity restatement and guarantee payment – The City's opinion draws attention to Note 26 of the financial report which (a) discloses the 2020 financial impact of the initial application of accounting standards AASB 1059 from the associate entity and (b) discloses a guarantee payment made by the City subsequent to reporting date. The opinion is not modified in respect of this matter.
City of Vincent	Events occurring after the end of the reporting period – The City's opinion included an EoM drawing attention to Note 30 of the financial report, which discloses a payment made by the City subsequent to the reporting period. The opinion is not modified in respect of this matter. Restatement of comparative balances – The City's Opinion also includes an EoM drawing attention to Note 32 of the financial report which states that the amounts reported in the

Entity	Description of emphasis of matter paragraphs
	previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
City of Wanneroo	Associate entity restatement and guarantee payment – The City's opinion draws attention to Note 38 of the annual financial report, which discloses (a) the 2020 financial impact of the initial application of accounting standard AASB 1059 from the associate and (b) a guarantee payment made by the City subsequent to reporting date. The opinion is not modified in respect of this matter.
Mindarie Regional Council	Contingent liability – The Council's opinion included an EoM drawing attention to Note 34 which disclosed a contingent liability relating to the Tamala Park Waste Management Facility site. The opinion is not modified in respect of this matter.
Pilbara Regional Council	Basis of accounting – The Council's opinion draws attention to Note 1(a) of the annual financial report, which discloses that the Council has decided to wind up. Consequently, the annual financial report has been prepared on a liquidation basis. The opinion is not modified in respect of this matter.
Rivers Regional Council	Basis of accounting – The Council's opinion draws attention to Note 1(a) of the annual financial report, which discloses that the Council has decided to wind up after ministerial approval is received for the formation of a regional subsidiary. Consequently, the annual financial report has been prepared on a liquidation basis. The opinion is not modified in respect of this matter.
Shire of Carnamah	Restatement of comparative balances – The Shire's opinion draws attention to Note 24 (correction of error) and subsequently Note 27 (financial ratios) to the financial report which states that the amounts reported in the previously issued 30 June 2020 (including comparative figures) financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Christmas Island	Restatement of comparative balances – The Shire's opinion draws attention to Note 29 of the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Cocos (Keeling) Islands	Restatement of comparative balances – The Shire's opinion draws attention to Note 25 of the financial report which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Coorow	Restatement of comparative figures – The Shire's opinion draws attention to Note 31 to the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.

Entity	Description of emphasis of matter paragraphs
Shire of East Pilbara	Restatement of comparative figures – The Shire’s opinion draws attention to Note 29 of the financial report which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Gingin	Restatement of comparative figures – The EoM paragraph draws attention to Note 30 to the financial statements which states that the amounts reported in the previously issued 30 June 2020 annual financial report have been restated and disclosed as comparatives in this annual financial report. The opinion is not modified in respect of this matter.
Shire of Halls Creek	Restatement of comparative balances – The Shire’s opinion draws attention to Note 26 to the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Harvey	Recording of joint venture – The EoM paragraph draws attention to Note 26 to the financial statements which states that the Shire’s equity share in the Investment in Associate is still being negotiated and therefore cannot be reliably estimated at this point of time. Consequently, the investment is not currently reflected in the financial statements. The opinion is not modified in respect of this matter.
Shire of Meekatharra	Basis of accounting – The EoM paragraph draws attention to Note 1 to the financial report, which describes the basis for accounting. The financial report has been prepared for the purpose of fulfilling the Shire’s financial reporting responsibilities under the Act. Regulation 17A of the FM Regulations requires a local government to measure vested improvements at fair value and the associated vested land at zero cost. This is a departure from AASB 16 Leases which would have required the entity to measure the vested improvements also at zero cost. The opinion is not modified in respect of this matter.
Shire of Mingenew	Basis of accounting – The Shire’s opinion included an EoM drawing attention to Note 28 of the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Shire of Plantagenet	Restatement of comparative balances – The Shire’s opinion draws attention to Note 29 to the financial statements which states that the amounts reported in the previously issued 30 June 2020 financial report have been restated and disclosed as comparatives in this financial report. The opinion is not modified in respect of this matter.
Tamala Park Regional Council	Basis of accounting – The Council’s opinion draws attention to Notes 1 and 10 to the financial report, which describes the basis for accounting. The financial report has been prepared for the purpose of fulfilling the Council’s financial reporting responsibilities under the Act. Regulation 17A of the

Entity	Description of emphasis of matter paragraphs
	<p>FM Regulations requires a local government to measure vested improvements at fair value and the associated vested land at zero cost. This is a departure from AASB 16 Leases which would have required the entity to measure the vested improvements also at zero cost. The opinion is not modified in respect of this matter.</p>
<p>Town of Victoria Park</p>	<p>Basis of accounting – The Town’s opinion draws attention to Note 36 of the annual financial report, which (a) discloses the 2020 financial impact of the initial application of accounting standards AASB 1059 from the associate entity and (b) discloses a guarantee payment made by the Town subsequent to reporting date. The opinion is not modified in respect of these matters.</p>

Source: OAG

Appendix 5: Material matters of non-compliance with legislation

Issue	Finding
Financial ratios not reported	<p>Twenty-eight entities did not report the Asset Renewal Funding Ratio, mostly for the three years, 2020, 2019 and 2018, in their annual financial report as required by FM Regulation 50(1)(c). Reasons for non-reporting included:</p> <ul style="list-style-type: none"> management had not updated the asset management plan for a number of years planned capital renewals and required capital expenditures were not estimated as required to support the long term financial plan and asset management plan respectively management could not confirm the reliability of the available information on planned capital renewals and required capital expenditure information on planned capital renewals and required capital expenditure over a 10 year period was not available.
Quotes not obtained or no evidence retained	<p>At 22 entities there was inadequate or no evidence that enough quotations were obtained to test the market and no documentation to explain why other quotes were not sought. This practice increases the likelihood of not receiving value for money in procurement and/or favouritism of suppliers.</p>
Controls over accounting journal entries	<p>At 13 entities we found that accounting journal entries were often posted to the financial ledger with no evidence of independent review and approval by another person. Accounting journals can represent significant adjustments to previously approved accounting transactions and could result in, for example, one type of expenditure being re-coded to another type of expenditure. If not closely controlled, unauthorised journals could result in errors in financial reports or fraud. Journals should therefore be subject to independent review.</p>
Financial management review not completed	<p>At 13 entities the Financial Management Review was not completed every three years as required by Regulation 5(2)(c) of the FM Regulations. This regulation requires the CEO to undertake reviews of the appropriateness and effectiveness of the financial management systems and procedures of the local government regularly (and not less than once in every three financial years) and report those reviews to the local government.</p>
Masterfile changes and access	<p>At 12 entities changes made to the supplier master files were not independently reviewed and approved by a staff member. This increases the risk of unauthorised changes to key information and may make fraud or error more difficult to detect.</p>
Bank reconciliation process incomplete	<p>At 12 entities bank reconciliation processes of their municipal, reserve and/or trust account were not prepared, had long</p>

Issue	Finding
	outstanding unreconciled items and/or there was no independent review by management.
Procurement without purchase orders	At seven entities purchase orders were not prepared or were prepared after the suppliers' invoices were received.
No fixed asset reconciliation	At seven entities monthly reconciliations of fixed assets were not completed for the majority of the financial year. This increased the risk of misstatements, fraud and errors not being detected in a timely manner.
Payroll and human resources findings	<p>Several findings of payroll and employment non-compliance were also reported at seven entities. Some examples include:</p> <ul style="list-style-type: none"> • a lack of segregation of duties as the staff member preparing the payroll and entering new employees into the system is also the first authoriser of payroll payments through the shire's bank account, increasing the risk of unauthorised or fraudulent transactions • payroll reconciliations not performed regularly to reconcile the payroll report to the general ledger • no formal policy or procedure in place to remove user access on termination of staff. This could lead to inappropriate access to shire information and possible financial loss to the shire if not addressed.
Procurement without appropriate segregation of duties	At five entities we identified the same officer requisitioned, approved and raised the purchase order then also approved the associated invoice payment for a significant proportion of sampled purchase transactions.
Review not performed of risk management, internal control and legislative compliance	At four entities a review of systems and procedures in relation to risk management, internal control and legislative compliance was not completed at least once every three years as required by LG Audit Regulation 17.
Depreciation	Three entities did not have adequate controls to determine if depreciation was being correctly calculated and recorded for certain infrastructure assets. This increased the risk of expenses being understated and assets being overstated.
Accessed monies in reserve to fund operations	At one entity, a review of the cash and cash equivalents account revealed that the entity has accessed monies in reserve accounts to fund its operations. This is a breach of section 6.11(2)(a) of the LG Act, which requires the entity to give one month's local public notice if the money in a reserve account is proposed to be used for another purpose.
Procurement without tender	At one entity, we identified no public tenders were invited for a contract with the value above \$250,000 as required by section 11(1) of the Local Government (Functions and General) Regulations 1996. This increases the likelihood of not receiving value for money in procurement, and/or favouritism of suppliers.
Records not presented to Council meetings as required by FM Regulations	At one entity the statements of financial activity for the months of October and December 2020 were not prepared and presented to Council as required by section 6.4 of the LG Act and Regulation 34(1) of the FM Regulations.

Issue	Finding
<p>Other procurement and miscellaneous findings</p>	<p>We reported other instances of non-compliance with procurement policies and procedures such as:</p> <ul style="list-style-type: none"> • credit card transactions were not separately listed in the payments submitted to council each month as required by Regulation 13(1) of the FM Regulations. We also found an instance where staff allocated a credit card did not sign the credit card acknowledgement form prior to using the card • insufficient documentation to demonstrate and evidence the on-going management of contract progress and supplier performance from contract award through to completion for its infrastructure projects • at one entity the purchasing policy is silent on declaring conflicts of interest in relation to open tenders. It has also not been reviewed since 2011. This entity’s buying goods and service’s manual, supporting the purchasing policy, has not been reviewed since 2012 • non-compliance with the <i>Unclaimed Money Act 1990</i> that requires monies over \$100 be transferred to the Department of Treasury if they have been held for six years without being returned to owners.
<p>General computer control findings</p>	<p>In depth findings of our information system audits at a selection of 45 entities are detailed in our <i>Information Systems Audit Report 2022 - Local Government Entities</i>, Report 22, tabled on 28 June 2022.</p> <p>In 2020-21, we reported 358 control weaknesses to 45 entities. Ten percent (37) of these rated as significant and 71% (254) as moderate. As these weaknesses could significantly compromise the confidentiality, integrity and availability of information systems, the entities should act promptly to resolve them.</p>

Source: OAG

Appendix 6: Certifications issued

In addition to annual auditor's reports, some entities needed to acquit moneys received from other sources under grant agreements or other legislation. We issued the following 275 certifications on statements of income and expenditure of entities, to help them discharge their financial reporting obligations, some being for Commonwealth grants.

Entity	Date certification issued	
	Roads to Recovery Funding under the <i>National Land Transport Act 2014</i>	Local Roads and Community Infrastructure Program
City of Albany	28/10/2021	29/10/2021
City of Armadale	16/11/2021	16/11/2021
City of Bayswater	29/10/2021	In progress
City of Belmont	26/10/2021	26/10/2021
City of Bunbury	29/10/2021	29/10/2021
City of Busselton	25/10/2021	26/10/2021
City of Canning	28/10/2021	28/10/2021
City of Cockburn	28/10/2021	29/10/2021
City of Fremantle	27/10/2021	In progress
City of Gosnells	29/10/2021	29/10/2021
City of Greater Geraldton	28/10/2021	28/10/2021
City of Joondalup	25/10/2021	26/10/2021
City of Kalamunda	26/10/2021	29/10/2021
City of Kalgoorlie-Boulder	21/03/2022	23/02/2022
City of Karratha	27/10/2021	27/10/2021
City of Kwinana	28/10/2021	29/10/2021
City of Mandurah	5/11/2021	5/11/2021
City of Melville	19/11/2021	19/11/2021
City of Nedlands	29/10/2021	In progress
City of Perth	26/10/2021	29/10/2021
City of Rockingham	29/10/2021	29/10/2021
City of South Perth	29/10/2021	1/11/2021
City of Subiaco	29/10/2021	29/10/2021
City of Stirling	8/10/2021	18/01/2021
City of Swan	29/10/2021	29/10/2021
City of Vincent	29/10/2021	28/10/2021
City of Wanneroo	28/10/2021	29/10/2021
Shire of Ashburton	7/12/2021	13/12/2021
Shire of Augusta-Margaret River	28/10/2021	18/02/2022
Shire of Beverley	28/10/2021	18/11/2021

Entity	Date certification issued	
	Roads to Recovery Funding under the <i>National Land Transport Act 2014</i>	Local Roads and Community Infrastructure Program
Shire of Boddington	2/02/2022	2/02/2022
Shire of Boyup Brook	29/10/2021	In progress
Shire of Bridgetown-Greenbushes	5/11/2021	22/11/2021
Shire of Brookton	5/11/2021	31/01/2022
Shire of Broome	26/10/2021	26/10/2021
Shire of Broomehill-Tambellup	In progress	In progress
Shire of Bruce Rock	27/10/2021	27/10/2021
Shire of Capel	8/12/2021	8/12/2021
Shire of Carnamah	29/10/2021	29/10/2021
Shire of Carnarvon	12/11/2021	16/11/2021
Shire of Chapman Valley	25/10/2021	28/10/2021
Shire of Chittering	26/05/2022	29/04/2022
Shire of Christmas Island	28/10/2021	18/11/2021
Shire of Cocos (Keeling Islands)	1/12/2021	7/12/2021
Shire of Collie	16/11/2021	18/11/2021
Shire of Coolgardie	14/12/2021	8/02/2022
Shire of Coorow	1/12/2021	16/11/2021
Shire of Corrigin	27/10/2021	27/10/2021
Shire of Cranbrook	26/10/2021	30/09/2021
Shire of Cuballing	28/10/2021	4/11/2021
Shire of Cue	11/11/2021	17/12/2021
Shire of Cunderdin	2/05/2022	2/03/2022
Shire of Dalwallinu	28/10/2021	8/03/2022
Shire of Dandaragan	29/10/2021	29/10/2021
Shire of Dardanup	27/04/2022	27/04/2022
Shire of Denmark	28/10/2021	29/10/2021
Shire of Derby-West Kimberley	30/03/2022	17/06/2022
Shire of Donnybrook-Balingup	9/11/2021	15/12/2021
Shire of Dowerin	11/11/2021	15/12/2021
Shire of Dumbleyung	26/10/2021	28/10/2021
Shire of Dundas	3/12/2021	6/05/2022
Shire of East Pilbara	3/05/2022	In progress
Shire of Esperance	23/03/2022	23/03/2022
Shire of Exmouth	25/10/2021	28/10/2021
Shire of Gingin	31/10/2021	22/11/2021

Entity	Date certification issued	
	Roads to Recovery Funding under the <i>National Land Transport Act 2014</i>	Local Roads and Community Infrastructure Program
Shire of Gnowangerup	29/10/2021	29/10/2021
Shire of Goomalling	29/10/2021	22/04/2022
Shire of Halls Creek	19/11/2021	29/10/2021
Shire of Harvey	1/11/2021	26/11/2021
Shire of Irwin	29/10/2021	26/10/2021
Shire of Jerramungup	12/10/2021	23/12/2021
Shire of Katanning	3/11/2021	22/12/2021
Shire of Kellerberrin	26/10/2021	23/08/2021
Shire of Kent	29/10/2021	26/10/2021
Shire of Kojonup	26/10/2021	28/10/2021
Shire of Kondinin	28/10/2021	29/10/2021
Shire of Koorda	5/11/2021	31/03/2022
Shire of Kulin	9/12/2021	6/12/2021
Shire of Lake Grace	29/10/2021	26/11/2021
Shire of Laverton	29/10/2021	13/12/2021
Shire of Leonora	26/10/2021	3/11/2021
Shire of Manjimup	28/10/2021	17/02/2022
Shire of Meekatharra	25/10/2021	27/10/2021
Shire of Menzies	21/12/2021	17/02/2022
Shire of Merredin	28/06/2022	29/06/2022
Shire of Mingenew	27/10/2021	29/10/2021
Shire of Moora	22/12/2021	In progress
Shire of Morawa	28/10/2021	28/10/2021
Shire of Mount Magnet	28/10/2021	29/10/2021
Shire of Mount Marshall	27/10/2021	27/10/2021
Shire of Mukinbudin	25/02/2022	25/02/2022
Shire of Mundaring	29/10/2021	13/12/2021
Shire of Murchison	22/03/2022	21/03/2022
Shire of Murray	28/10/2021	29/10/2021
Shire of Nannup	8/12/2021	In progress
Shire of Narembeen	28/10/2021	28/10/2021
Shire of Narrogin	26/10/2021	26/10/2021
Shire of Northam	3/11/2021	3/11/2021
Shire of Northampton	26/10/2021	1/12/2021
Shire of Nungarin	29/10/2021	29/10/2021

Entity	Date certification issued	
	Roads to Recovery Funding under the <i>National Land Transport Act 2014</i>	Local Roads and Community Infrastructure Program
Shire of Ngaanyatjarraku	28/10/2021	29/10/2021
Shire of Peppermint Grove	In progress	In progress
Shire of Perenjori	28/10/2021	28/10/2021
Shire of Pingelly	29/10/2021	29/10/2021
Shire of Plantagenet	26/10/2021	27/10/2021
Shire of Quairading	8/11/2021	25/03/2022
Shire of Ravensthorpe	21/12/2021	21/12/2021
Shire of Sandstone	3/11/2021	In progress
Shire of Serpentine-Jarrahdale	1/11/2021	1/11/2021
Shire of Shark Bay	25/10/2021	26/10/2021
Shire of Tammin	26/10/2021	29/10/2021
Shire of Three Springs	29/10/2021	2/11/2021
Shire of Toodyay	29/10/2021	29/10/2021
Shire of Trayning	27/10/2021	29/10/2021
Shire of Upper Gascoyne	27/10/2021	27/10/2021
Shire of Victoria Plains	17/11/2021	17/11/2021
Shire of Wagin	29/10/2021	31/03/2022
Shire of Wandering	3/11/2021	5/11/2021
Shire of Waroona	28/10/2021	28/10/2021
Shire of West Arthur	29/10/2021	29/10/2021
Shire of Westonia	27/10/2021	25/02/2022
Shire of Wickpin	29/10/2021	16/05/2022
Shire of Williams	29/10/2021	23/12/2021
Shire of Wiluna	In progress	In progress
Shire of Wongan-Ballidu	29/10/2021	In progress
Shire of Woodanilling	23/02/2022	13/05/2022
Shire of Wyalkatchem	26/10/2021	28/10/2021
Shire of Yalgoo	22/03/2022	22/03/2022
Shire of Yilgarn	24/11/2021	23/11/2021
Shire of York	27/10/2021	27/10/2021
Shire of Wyndham-East Kimberley	6/05/2022	In progress
Town of Bassendean	29/10/2021	29/10/2021
Town of Cambridge	28/10/2021	1/11/2021
Town of Claremont	3/11/2021	10/11/2021
Town of Cottesloe	26/10/2021	21/12/2021

Entity	Date certification issued	
	Roads to Recovery Funding under the <i>National Land Transport Act 2014</i>	Local Roads and Community Infrastructure Program
Town of East Fremantle	8/10/2021	Deferred*
Town of Mosman Park	29/10/2021	29/10/2021
Town of Port Hedland	4/04/2022	28/02/2022
Town of Victoria Park	30/10/2021	30/10/2021

Source: OAG

* Approval obtained from the Commonwealth to defer certification of financial statements

Entity	Date certification issued
Claims by administrative authorities – Pensioner deferments under the <i>Rates and Charges (Rebates and Deferments) Act 1992</i>	
City of Belmont	2/03/2022
City of Busselton	1/11/2021
City of Joondalup	2/11/2021
City of Kalamunda	8/12/2021
City of South Perth	2/11/2021
City of Vincent	10/11/2021
Shire of Dandaragan	17/01/2022
Shire of Narrogin	25/02/2022
Shire of York	21/12/2021
Town of Cambridge	4/01/2022
Town of Mosman Park	15/12/2021

Source: OAG

Entity certification	Date certification issued
Other certifications	
City of Kalamunda – Development Contribution Area 1 – Forrestfield Light Industrial Area Stage 1	8/12/2021
Shire of Brookton – Drought Communities Programme - Extension	17/09/2021
Shire of Dandaragan – Jurien Bay Civic Centre Outgoings	20/01/2022

Source: OAG

Appendix 7: Other opinions and certifications issued since 18 November 2021

State government entity opinions

Entity	Opinion relates to	Opinion issued
Albany Cemetery Board	Audit report on the Statement of Financial Position at 30 June 2021	15/12/2021
Bunbury Cemetery Board	Audit report on the Statement of Financial Position at 30 June 2021	4/02/2022
Kalgoorlie-Boulder Cemetery Board	Audit report on the Statement of Financial Position at 30 June 2020	21/12/2021
Kalgoorlie-Boulder Cemetery Board	Audit report on the Statement of Financial Position at 30 June 2021	21/02/2022

Source: OAG

State government entity certifications

The following certifications were for the year ended 30 June 2021. The statements prepared by management were confirmed and no adverse reports were issued.

Entity	Certification relates to	Date issued
Commissioner of Main Roads	Statement of amounts expended or retained for expenditure under the Land Transport Infrastructure Projects (<i>National Land Transport Act 2014</i>).	10/12/2021
Commissioner of Main Roads	Statement of amounts expended or retained for expenditure under the National Partnership on Infrastructure Projects in Western Australia.	10/12/2021
Department of Local Government, Sport and Cultural Industries	Statement of payments made to Local Governments under the <i>Local Government (Financial Assistance) Act 1995</i> .	26/11/2021

Source: OAG

Royalties for Regions certifications

Entity	Royalties for Regions approved project	Date issued
Department of Primary Industries and Regional Development	Gascoyne Foodbowl Land Release	3/02/2022
Department of Treasury	Governance of Royalties for Regions Program	3/12/2021
WA Country Health Service	Albany Radiation Oncology	29/11/2021
	Bunbury Hospital Redevelopment	29/11/2021
	Carnarvon Residential Aged Care Facility	29/11/2021
	Collie Hospital Upgrade	29/11/2021

Entity	Royalties for Regions approved project	Date issued
	Derby Community Health Service	29/11/2021
	Digital Innovation, Transport and Access to Care	29/11/2021
	Dongara Aged Care	29/11/2021
	Country Health Innovation – Emergency and Acute Workforce	29/11/2021
	Expand the Ear Bus Program	29/11/2021
	Geraldton Health Campus Redevelopment	29/11/2021
	Kalgoorlie Health Campus Magnetic Resonance Imaging Suite	29/11/2021
	Karratha Health Campus	29/11/2021
	Kimberley Mobile Dialysis Unit	29/11/2021
	Meet and Greet Unit	29/11/2021
	Newman Health Service Redevelopment Project	29/11/2021
	Nickol Bay Hospital Site	29/11/2021
	Onslow Health Service Redevelopment Project	29/11/2021
	Pilbara Health Initiative Phase 3	29/11/2021
	Remote Indigenous Health Clinics	29/11/2021
	Renal Dialysis Services	29/11/2021
	Renal Hostels	29/11/2021
	Residential Aged and Dementia Care Investment Program	29/11/2021
	Southern Inland Health Initiative – Stream 2a, 3 and 4	29/11/2021
	Tom Price Hospital Redevelopment	29/11/2021

Source: OAG

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2022-23 reports

Number	Title	Date tabled
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

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

www.audit.wa.gov.au



[@OAG_WA](https://twitter.com/OAG_WA)



Office of the Auditor General
for Western Australia