



APPENDICES

AUDIT & RISK COMMITTEE MEETING

To Be Held

Wednesday, 13th September 2023
Commencing at 2.00pm

At

Shire of Dardanup
ADMINISTRATION CENTRE EATON
1 Council Drive - EATON

This document is available in alternative formats such as:

- ~ Large Print
- ~ Electronic Format [disk or emailed]
Upon request.

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Western Australian Auditor General – Schedule of Reports

RISK THEME PROFILE:

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

RISK ASSESSMENT CONTEXT: Strategic

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



Report 23: 2022-23 | 14 June 2023

FORENSIC AUDIT

Contractor Procurement – Data Led Learnings



**Office of the Auditor General
Western Australia**

Audit team:

Carl Huxtable
Forensic Audit team

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

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

© 2023 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: Thanakorn.P/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Contractor Procurement – Data Led Learnings

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

CONTRACTOR PROCUREMENT – DATA LED LEARNINGS

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

This forensic audit was an exercise to develop our forensic data analytics methodology, using contractor procurement data from the Public Transport Authority to seek to identify red flags that could indicate undisclosed relationships or corrupt procurement practices.

I wish to acknowledge the entity's staff for their cooperation with this audit work.

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

CAROLINE SPENCER
AUDITOR GENERAL
14 June 2023

Contents

Auditor General’s overview 5

Executive summary 6

 Introduction 6

 Background 6

 Conclusion 7

Learnings..... 8

 Procurement processes vulnerable to favouritism or bias..... 8

 Conflict of interest management..... 9

 Due diligence on suppliers 9

 Contract costs and contract splitting 11

Recommendations..... 13

Audit focus and scope 15

Auditor General's overview

Significant amounts are invested annually across the Western Australian public sector to deliver core services to our community, and we expect the procurement of goods and services to be based on the relationship between value for money, timeliness and quality. The risk of public funds being diverted by fraud or corruption increases when we add influence to this equation, especially when the decision on what to buy, how much and who from can be at the discretion of one individual. There is a constant vulnerability to bias and favouritism when engaging third party contractors and independence, actual or perceived, can be difficult to navigate where suppliers are:



- limited (providing specialist services)
- proven to deliver as a result of prior engagement by the entity
- consulted in advance to ensure the procurement request seeks the appropriate goods and services.

Mitigating this vulnerability requires a well-structured, sustained approach by all State government entities, particularly those engaging in high volume procurement of contractors. Robust policies, controls and well targeted analytics is important.

The Public Transport Authority (PTA) has previously identified and reviewed anomalies within its contractor data and focused attention over recent years on improving the probity of its procurement activities. This work led to the removal of a qualified controls audit opinion for the PTA for the 2021-22 financial year.

The PTA informing us of these anomalies allowed us to assess the data analytic capability of our forensic audit function and test a key model intended for regular deployment in future audits, searching for contractor fraud and corruption red flag indicators. I am pleased to note, in addition to anomalies identified by the PTA, our tools and techniques identified additional red flags and contracts for review.

Any data analytic red flag represents unexpected or unusual results which may have legitimate reasons for sitting outside the curve. A flag does not, of itself, indicate fraud or corruption. Deeper review of 'red flags' is required. In this audit, we noted historical vulnerabilities in conflict-of-interest processes, due diligence and contract management. Our review did not give rise to a suspicion of fraud or corruption, but did highlight procedural, mathematical and documentary gaps that could have been exploited by those dishonestly inclined.

We recognise and thank the PTA for open, honest and frank dialogue during the audit, without which our capability could not be tested and these lessons could not be shared.

While corrective steps have been taken within the PTA to resolve the historical vulnerabilities we identified, the Western Australian public sector can benefit by us sharing those experiences.

Executive summary

Introduction

This audit was an exercise to develop our forensic data analytics methodology, using contractor procurement data from the Public Transport Authority (PTA) within the Network and Infrastructure division (N&I) and Office of Major Transport Infrastructure Delivery (OMTID), to seek to identify red flags that could indicate undisclosed relationships or corrupt procurement practices.

We are encouraged by the PTA's self-identification and detailed review of various irregularities in the procurement process.

Our review covered a five-year period from 1 July 2016 to 30 June 2021. We note that, in addition to legislatively driven change including in the *Procurement Act 2020*, the PTA has advised of other internal reforms to policy, process and control.

Background

The State Government currently has a multi-billion dollar road and rail transport infrastructure investment program, which includes new works and maintenance on existing assets.

Transport portfolio entities engage with an extensive network of contractors. In 2021-22, the PTA spent \$367 million on contractors.¹ This level of spending, coupled with the portfolio's broad and diverse procurement, creates potential risks and vulnerabilities to fraud and corruption.

The OMTID was established in May 2020 as a centre of excellence between the PTA and Main Roads Western Australia for major project delivery.

The PTA's N&I manages, maintains and upgrades the metropolitan railway infrastructure.

The PTA has a sound level of awareness of risks in its operations, including many procurement risks. The PTA informed our Financial Audit team that it had previously considered its procurement process in the N&I, reviewed the issues identified in Table 1 and made changes to their process to mitigate these risks. This information aided the scope of our forensic audit work.

Issue	Description
Suppression of bids	Contractors collude with one another to determine who will not bid or will withdraw from the process.
Shadow bidding	Contractors collude with one another and agree to submit inadequate bids.
Rotation of bidding among vendors	Contractors collude with one another to alternate the business among themselves and subcontract to the unsuccessful contractors.

Source: OAG based on PTA information

Table 1: Procurement risks identified by the PTA

Our initial data testing and review of procurement systems identified high risk PTA contractors within OMTID and N&I.

¹ Public Transport Authority, [Annual Report 2021-2022](#), PTA, Perth, 2022, p 99.

Entities use many types of contracting arrangements to perform a number and range of services and functions. Contractors may be at true arms-length or embedded in the operations of an entity in a role akin to an employee, or any range in between. The Corruption and Crime Commission commented on the nature of embedded contractors:

There is a serious misconduct risk in the wider public sector where there is insufficient oversight of contractors embedded in public agencies on rolling short term contracts.

Embedded contractors typically work within public agencies for an extended period alongside public officers, and in some instances, performing the same role as a public officer.

There is a risk embedded contractors may act in their own self-interest and not for the public benefit. A contractor may 'drag' projects out to ensure they have ongoing work, or favour other external parties by influencing referrals of work from public agencies. The insecurity of a contractor's position might, perhaps, be felt increasingly keenly with the passage of time.

The fees paid to embedded contractors are public monies, and as such, there should be appropriate mechanisms in place to ensure the work performed and the conduct of the contractors adheres to the same standards of propriety required of all public officers. The Commission considers the community would expect this level of accountability when public monies are expended, and especially when contractors are performing what would otherwise be a public officer function.²

Our examination of the PTA was focused on the risks associated with contractor procurement and contract management.

Data analytics within our forensic audit function assessed contractors within N&I and OMTID and identified 127 awarded contracts for further interrogation, of which we only examined contractors not already reviewed by the PTA.

Conclusion

It is pleasing to see the identification of risk and response by the PTA. While not indicative of wrongdoing, we found fraud and corruption vulnerabilities that could have been exploited in the PTA's previous procurement practices through instances of undeclared conflicts of interest, unmanaged conflicts of interest, inadequate supplier due diligence and contract management issues.

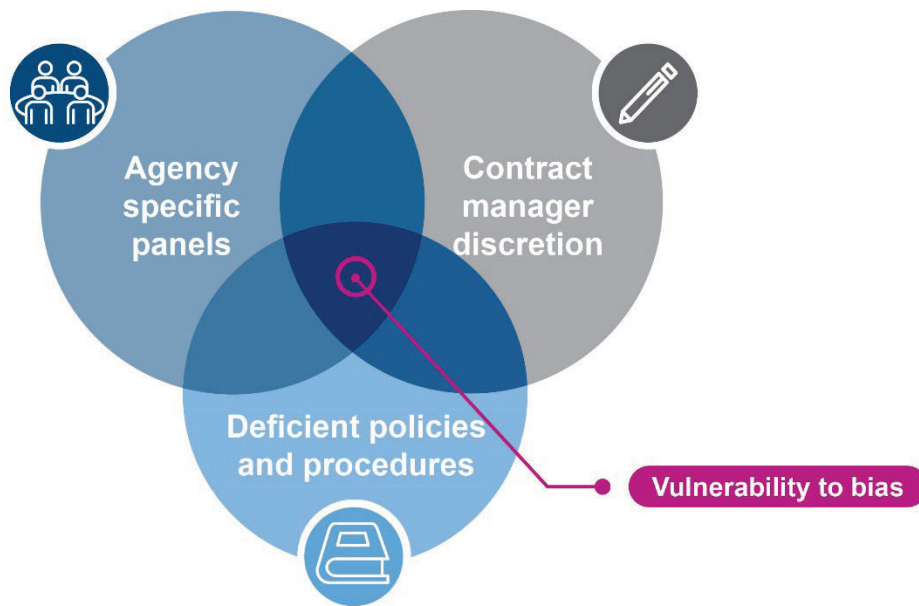
² Corruption and Crime Commission, *A report on corrupt procurement practices and conduct in the Department of Communities*, CCC, Perth, 2022, p. 53.

Learnings

Procurement processes vulnerable to favouritism or bias

State government entities are able to establish agency specific panels and these are supported by State procurement guidelines.³ Panels are established for consistent, large volumes of goods or services. All suppliers appointed to the panel can deliver the required good or service. An example of an agency specific panel being manipulated was identified by the Corruption and Crime Commission in a 2022 report on individuals within the Department of Communities.⁴

Guidance should be provided, and decisions clearly documented, when work allocation is left to the discretion of an individual. Without these, there is a risk that bias or personal relationships may influence the allocation of work. This increases the risk of fraud or corruption occurring.



Source: OAG

Figure 1: Agency specific panel's bias risk

Case study 1: Agency specific panels

At the PTA during the period examined, direct quotations were only needed from one supplier on the agency specific panel if the value of work was estimated to be below \$150,000. The contract manager had the discretion to select which supplier to approach for a direct quote. We were unable to find documented policies or procedure, or case-based records, outlining relevant considerations when exercising this discretion.

The PTA advised that its policy is contractors listed on the panel are not guaranteed work and it has implemented:

³ Department of Finance, [Agency Specific Panels](#), Government of Western Australia website, n.d., accessed 16 May 2023.

⁴Corruption and Crime Commission, *A report on corrupt procurement practices and conduct in the Department of Communities*, CCC, Perth, 2022, pp 8-10.

- updates to its procurement rules and guidelines with the introduction of the *Procurement Act 2020*
- a requirement for reviews by senior procurement staff to ensure that the appropriate levels of due diligence are undertaken
- panel buying transferred to a specialist branch
- regular contract reviews (end of contract or during variation consideration).

Conflict of interest management

If conflicts of interest, including perceived conflicts, are not declared and appropriately managed, there is a risk that procurement is influenced in such a way that fraud or corruption occurs or value for money is not achieved.

The risk of influence in the procurement environment increases when there are only a handful of companies providing specialised services.

Case study 2: Conflict of interest declarations

During some of the period examined by our review the PTA could not provide conflict of interest forms for a number of staff on evaluation panels. There were no forms for 16 of the contracts we examined and for three evaluation panels we found the declarations lacked disclosure of perceived conflicts.

The three perceived conflicts related to panel members also being listed as a referee on a supplier's submission. The PTA advised it identified these conflicts and managed them by using an alternative referee. Whether a genuine conflict of interest exists or not, it could be perceived that the evaluation panel member could improperly or unduly influence the evaluation of suppliers for the contract so extra care must be taken to ensure unbiased procurement.

The PTA advised that the specialised nature of the work meant there was:

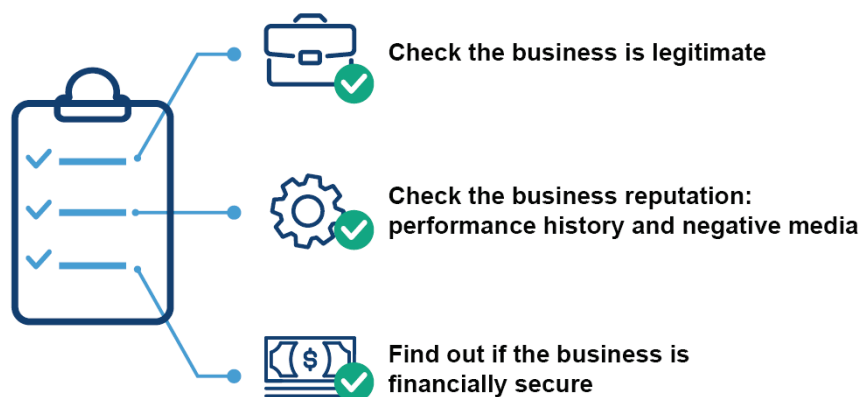
- a limited pool of suitable panel members
- most panel members would have an existing relationship with the tendering businesses.

The PTA also advised that, in September 2021, it launched an online conflict of interest form and portal and all declarations, management plans and review of management plans are now stored in an online repository.

Due diligence on suppliers

Good due diligence includes not just checking the Australian Business Number exists⁵, but also assessing other information sources to ascertain the financial stability, ability to perform and any reputational history of a supplier. This includes maintaining records justifying why new companies have been approached or reputational concerns need not be an issue. This increases transparency across an entity.

⁵ Checking for an Australian Company Number is not an indicator of a business registration – Australian Business Names and the Australian Business Register (which includes Australian Business Numbers and further details of holders) should be primary sources used in due diligence processes in conjunction with company searches.



Source: OAG

Figure 2: Supplier due diligence checklist

In the absence of appropriate due diligence there is the risk that an entity can be exposed to risks including the engagement of illegitimate or poor performing suppliers, non-delivery of services, overcharging for services and false invoicing. Not knowing your staff, customers and suppliers creates risks for any entity.

Australian Standard 8001:2021 *Fraud and Corruption Control* includes a number of points on managing the fraud and corruption risk by business associates⁶. Due diligence is a critical aspect of managing this risk.

Case study 3: Supplier due diligence

Our analysis identified one contract awarded to a supplier affiliated with an individual with drug trafficking convictions. The individual was a director of the supplier for one year, during which time it was engaged by the PTA. We identified this through open-source intelligence⁷. There is no record of the conviction being identified by the PTA.

The contract was originally awarded for \$90,200 and was procured by direct sourcing under the Aboriginal procurement exemptions. A subsequent variation took this total to \$282,700.

In another instance, a contractor was invited to quote only four days after it was registered on the Australian Securities and Investments Commission. There is no record justifying why a four-day old company was asked to quote or how it was deemed capable of providing the services given its infancy. Our examination identified that the supplier's director was a previous PTA contractor who had established a new business. While not documented, the PTA was of the view the contractor was capable of providing the services required.

The PTA advised that it conducts due diligence taking into account a variety of factors including the financial and operational risk presented by the suppliers. The PTA is satisfied with the level of due diligence being driven by the risk to the procurement, the entity or broader State Government.

⁶ Business associates includes, at section 1.4.4, suppliers, vendors, sub-contractors, joint venture partners and a number of other parties.

⁷ Open source intelligence is the practice of collecting information from published or otherwise publicly available sources.

The PTA regularly reviews its risk profile and this is taken into account when reviewing due diligence requirements.

The PTA also relies on the new debarment regime put in place by the Department of Finance as part the *Procurement Act 2020* to dictate which suppliers cannot be used by entities.

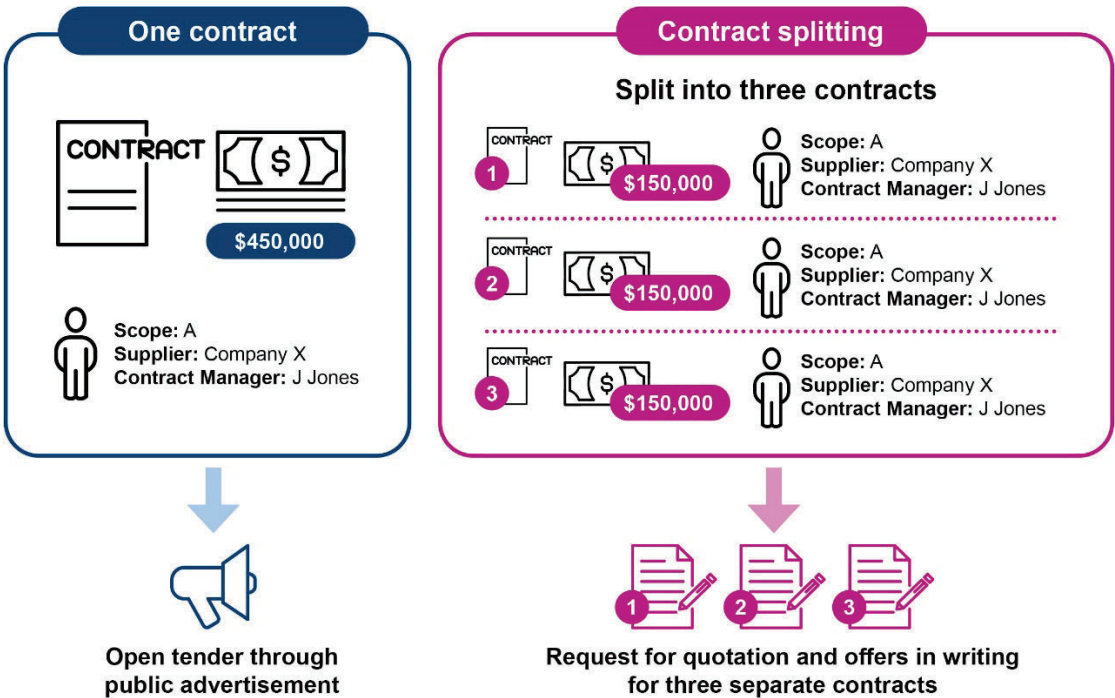
Contract costs and contract splitting

Excessive variations may be driven by market factors however may also indicate poor budgeting. Contracts requiring regular and repeated variations should be reviewed with remediation steps documented. Excessive variations may obscure the transparency of procurement but also increases the risk of fraudulent claims arising.

Accidental errors in procurement should be properly recorded, identifying the root cause for the error and lead to appropriate process improvement to prevent it happening again. Approving variations that do not reflect on the true cause of the error increase the risk of fraudulent variation claims being approved.

The Department of Finance notes a red flag or warning sign of procurement fraud is tender threshold avoidance, including contract splitting.⁸

Contract splitting is where one contract is divided into smaller quantities, amounts, phases or sub-contracts for the purpose of evading or circumventing competitive bidding and the requirements for alternative methods of procurement.



Source: OAG

Figure 3: Contract splitting

⁸ Department of Finance, [Red flags during pre-tender](#), Government of Western Australia website, 11 November 2020, accessed 16 May 2023.

Splitting contracts may sacrifice a fair and equitable procurement process for large value contracts and create additional costs where economies of scale could be achieved. Without a fair and equitable procurement process, there is a risk that value for money is not achieved, procurement is not competitive, preferred suppliers are being selected or fraud or corruption is occurring.

Case study 4: Contract costs and contract splitting

Our sample identified one contract in the PTA's records with 19 price variations over a five-year period, increasing the cost from approximately \$1.5 million to just over \$2.1 million (41% increase).

An error in the budget for another contract (one day per week instead of five) meant the contract cost was underestimated by 80% (\$84,480 instead of \$422,400) and the wrong procurement method was used. This error meant a significant variation was required only 11 weeks into what was meant to be an initial 46-week contract.

The variation stated that 'the contract was based on a budget of 505 hours' however:

- contract submissions provided hourly rates, not total cost or hours required
- the budget (which was 80% understated) showed 384 hours
- the request for quote estimated 1,840 hours.⁹

We also noted instances where contract managers created multiple separate contracts for similar goods or services. For example, similar services were required at three different locations. The PTA established three standalone contracts with consecutive contract numbers, awarded to the same supplier by the same contract manager on the same date.

The PTA advised that it has implemented a rigorous review approach to all contract variations to ensure that extending the contract reflects the best decision for the entity and will still result in value for money being received for the State Government.

The PTA also advised that it provides continued education and training with respect to the cost estimation in order to award contracts for the appropriate value the first time. More prescriptive information is being asked in the development of contract management plans which should also assist contract managers identify where the risk of variations might need to be considered in the procurement.

To encourage greater accuracy, the PTA is also implementing a process for pre-procurement estimates to encourage greater accuracy in understanding potential costs of services.

⁹ The calculation of 505 hours is arrived at by dividing the incorrect budget / contract award amount of \$84,480 by the winning hourly rate. This equates to around 10.97 hours per week where the request for quote required 'full time' for 46 weeks.

Recommendations

All State government entities should review their procurement and contract management arrangements and the fraud and corruption risks they present, this includes:

1. ensuring that conflicts of interest, including perceived conflicts, are declared, independently reviewed and recorded. Develop and document management plans that mitigate the risks associated with any perceived or actual conflicts identified
2. conducting due diligence on all suppliers that are awarded a contract and embed a practice of further enquiry where results conflict with standard expectations
3. reviewing contract management processes including contract variations and contract costing
4. developing controls that mitigate the risk of corruption occurring such as the regular rotation of contract managers and independent review of contract awards.

Response from the Public Transport Authority

The PTA would like to thank the Office of the Auditor General (OAG) for the opportunity to participate in one of the first of its type forensic data audit. The PTA is acutely aware of the risks and vulnerabilities that can exist within procurement processes within all agencies but especially within an agency with the volume and magnitude of spending of the PTA.

The PTA has taken the opportunity to review its procurement practices with the introduction of the *Procurement Act 2020* and was pleased that the recommendations identified by the OAG have already been implemented by the PTA.

While no process can be infallible, through continuous education and vigilance the PTA is working towards ensuring that the risks associated with procurement have been mitigated to as low as reasonably practicable.

The PTA acknowledges and appreciates the time spent by the staff from the OAG in getting to know and understand the PTA's business and operations, which ultimately led to this report – which is hopefully a constructive and beneficial report for all agencies.

The PTA looks forward to working with the OAG in a similar fashion in the future.

Audit focus and scope

Our objective was to develop our forensic data analytics capability, using contractor procurement data. Our focus was to:

- Identify undisclosed conflicts of interest between entity employees and vendors that had been awarded contracts.
- Identify links between vendors engaged in competitive quote submissions that may have compromised procurement processes.

This audit focused on procurement within the Public Transport Authority Network and Infrastructure division (for the period 1 July 2016 to 30 June 2021) and the Office of Major Transport Infrastructure Delivery division (for the period 1 May 2020 to 30 June 2021) jointly operated by PTA and MRWA.

Selecting areas for a forensic audit does not mean we suspect fraud or corruption is occurring; however, our audits are targeted by the combination of various fraud risk factors. Our intent is, preferably, to identify vulnerabilities that can be eliminated before fraud has occurred.

Profiling of procurement patterns and spend was used to identify high risk vendors and commissioning staff. Highly probable exceptions were identified for further investigation.

Forensic testing methods included but were not limited to:

- detailed data analytics on contract metrics
- data matching across data sets to uncover conflicts of interests
- examination of documents including requests for quote, tenders, supplier responses, contracts, variations documentation and payments data
- reviewing panel selection and make up of panel members.

This was an independent forensic audit, conducted under section 18 of the *Auditor General Act 2006*. The approximate cost of undertaking the audit and reporting was \$510,000.

This page is intentionally left blank

Auditor General's 2022-23 reports

Number	Title	Date tabled
22	Effectiveness of Public School Reviews	24 May 2023
21	Financial Audit Results – State Government 2021-22 – Part 2: COVID-19 Impacts	3 May 2023
20	Regulation of Air-handling and Water Systems	21 April 2023
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation of Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
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



Office of the Auditor General
for Western Australia



Report 24: 2022-23 | 14 June 2023

BETTER PRACTICE GUIDE

Security Basics for Protecting Critical Infrastructure from Cyber Threats



**Office of the Auditor General
Western Australia**

Audit team:

Aloha Morrissey
Kamran Aslam
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.

© 2023 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: Panimoni/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Security Basics for Protecting Critical
Infrastructure from Cyber Threats**

Report 24: 2022-23
14 June 2023

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

SECURITY BASICS FOR PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER THREATS

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*.

This better practice guide aims to help Western Australian public sector entities better manage cyber security threats to their critical infrastructure. The guide focuses on better practice principles to safeguard critical operational technology and has been informed by this Office's recent audit work on this topic.

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

CAROLINE SPENCER
AUDITOR GENERAL
14 June 2023

Contents

Auditor General’s overview 5

Part 1: Introduction 6

 1.1 About this guide 6

 1.2 Who should use this guide 6

 1.3 Background 6

Part 2: How to protect critical infrastructure from threats 11

 2.1 Identify and maintain an accurate inventory of important IT and OT assets11

 2.2 Develop a culture of security12

 2.3 Manage supply chain risks13

 2.4 Design a resilient network14

 2.5 Implement effective access management procedures15

 2.6 Manage vulnerabilities and maintain vigilance16

 2.7 Implement physical security.....17

 2.8 Be prepared for when things go wrong18

Appendix 1: Examples of common OT and IT communication protocols..... 19

Appendix 2: OT network segmentation – Purdue Model 20

Auditor General's overview

Cyber security is a critical concern across all industries as threats continue to evolve and pose significant threats. Australian organisations have seen an increase in successful cyber attacks in recent years. Of increasing concern, cyber criminals and nation states are also targeting critical infrastructure including power grids, water delivery systems, transport networks and communication systems.



These attacks pose a significant risk to our national security where consequences can impact health and safety, essential services and result in severe economic damage. As threats continue to grow in sophistication, effective strategies with multiple layers of defence over cyber and information security, supply chain, physical security and operational technology is required.

In response to growing cyber threats, governments worldwide are taking steps to improve cyber security measures and resilience of critical infrastructure. The Australian Government's amendments to the *Security of Critical Infrastructure Act 2018* is one such example.

Connectivity between IT and OT continues to blur network boundaries, it is therefore important to keep an eye on risks and defend against threats. Entities should remain vigilant, adapt to changing threat landscapes and collaborate to protect critical infrastructure. Security of critical infrastructure has been a key focus for my Office, and based on recent audit work in this area, this better practice guide aims to help entities manage cyber threats to their critical systems and infrastructure. Other public sector entities are also encouraged to use this guide to enhance their cyber resilience.

Part 1: Introduction

1.1 About this guide

This better practice guide aims to help Western Australian (WA) public sector entities better manage cyber security threats to their critical infrastructure¹. The guide focuses on better practice principles to safeguard critical operational technology (OT) and has been informed by this Office's recent audit work on this topic.

This is not intended to be an exhaustive document. Further guidance is available from the Cyber and Infrastructure Security Centre² and relevant standards. Some security standards are referred to in the Security of Critical Infrastructure Rules³ and include the:

- Australian Standard for Information Security AS ISO/IEC 27001:2015
- Essential Eight⁴ controls developed by the Australian Signals Directorate
- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity Capability Maturity Model by the Department of Energy of the United States of America
- 2020-21 AESCSF Framework Core by the Australian Energy Market Operator.

1.2 Who should use this guide

Entities who operate critical infrastructure, including those in the energy, water, transport, health sectors, and those responsible for maintaining critical communication infrastructure are encouraged to engage with the principles and practices in this guide. Other public sector entities are also encouraged to apply the principles as required to ensure the continuity and reliability of essential services.

1.3 Background

Every day, millions of Western Australians rely on critical infrastructure to access a range of essential services including public transport, clinical health services and the provision of water, gas and power to their homes and businesses.

Delivery of these services has increasingly moved away from historical manual processes towards reliance on information technology (IT) and OT systems working together (Figure 1). The benefits and efficiencies that arise from the use of IT and OT are numerous. They include the ability to remotely access and operate control systems used to deliver government services. For example, whenever we turn on a tap or a light, we access a

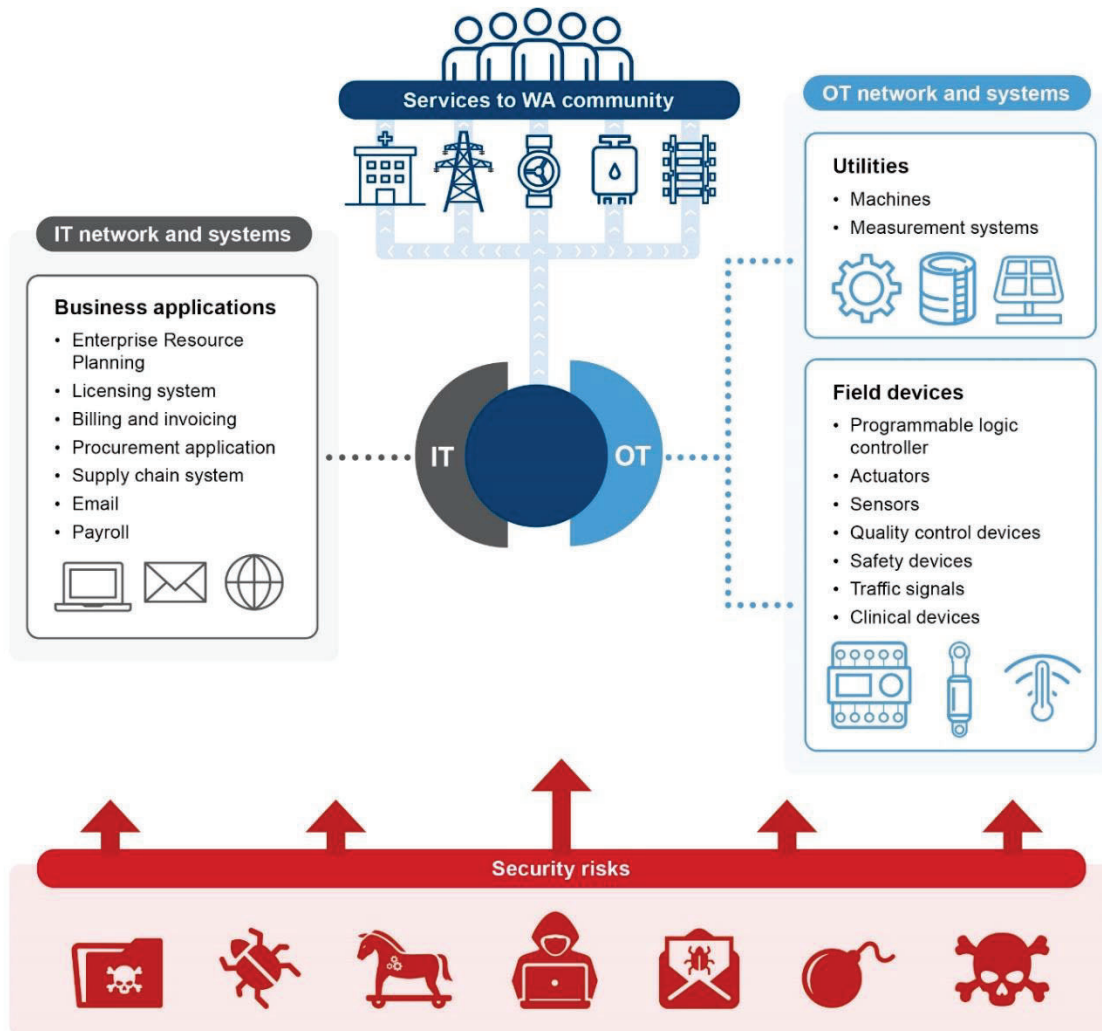
¹ Critical infrastructure is defined by the Cyber and Infrastructure Security Centre as those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.

² Australian Government Department of Home Affairs, '[Critical Infrastructure Resilience Strategy](#)', *Cyber and Infrastructure Security Centre*, 23 February 2023, accessed 8 June 2023.

³ Australian Government, '[Security of Critical Infrastructure \(Critical infrastructure risk management program\) Rules](#)', Federal Register of Legislation, 16 February 2023, accessed 8 June 2023.

⁴ Australian Government Australian Signals Directorate, '[Essential Eight Maturity Model](#)', *Australian Cyber Security Centre*, 24 November 2022, accessed 8 June 2023. These controls are mandated for WA State government entities by the [WA Government Cyber Security Policy](#). Although not mandatory for all government trading entities, the Essential Eight represent minimum controls for cyber security and should be considered.

complicated system underpinned by OT that includes industrial control systems, and supervisory control and data acquisition (SCADA⁵) systems.



Source: OAG

Figure 1: High level view of IT and OT convergence and risks

The interconnection of IT and OT exposes the control systems and the essential services they deliver to increased cyber risks. OT infrastructure is particularly targeted and protecting it presents unique challenges. OT software generally requires support from specialist suppliers, is often not secure by design and many traditional security controls cannot be applied to them. Unique and industry specific protocols (Appendix 1) drive OT networks, although common IT communication protocols are also used.

Inadequate security of OT systems can cause physical harm to people and damage to equipment that can lead to significant disruption and financial loss. For example, a cyber attack on a power grid could result in a widespread blackout, or a compromised industrial control system could cause a chemical plant to release hazardous substances. In comparison, a compromise of an IT business application could result in exposure of sensitive information or loss of information for decision making. Further examples of compromised IT and OT systems are listed below in Table 1.

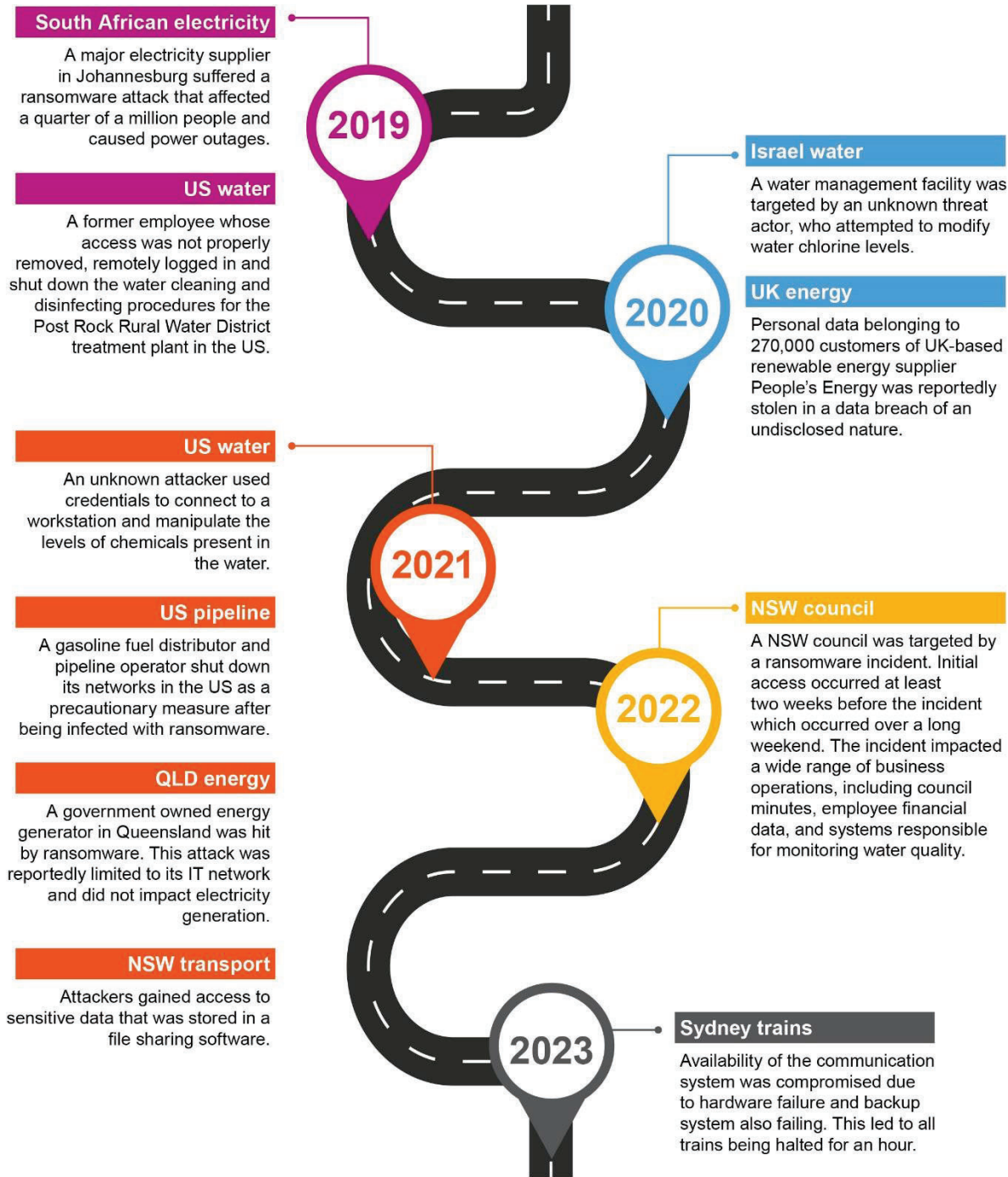
⁵ SCADA collectively refers to software and hardware (sensors, controllers, machines and computers) working together to deliver essential services.

Impact in OT environment	Impact in IT environment
Rail and road traffic signals may be compromised and result in crashes	A website which provides road congestion information may become unavailable
Power and water services to the public may not be delivered	Systems may not be available to establish new customer accounts, or prepare and process customer invoices
Loss of clinical health systems that support human life	Unavailability, theft or disclosure of private medical records
Systems that regulate the quantity of chemicals used to treat water may be disrupted	Systems may not generate and issue water bills to customers
Surgical systems and screens may not work during surgery	A medical appointment booking website may not be accessible

Source: OAG

Table 1: Examples of potential impacts of cyber incidents in IT and OT environments

Figure 2 provides examples of global incidents in the utilities sector from the last five years, highlighting the need for effective strategies to deter threats to critical infrastructure. Strategies should cover, but are not limited to, risk management, OT, people, supply chains, cyber and information security, and physical infrastructure.



Source: OAG based on publicly available information

Figure 2: Examples of critical infrastructure security breaches

(Appendix AAR: 8.1C)

In response to growing cyber threats to critical infrastructure, the Australian Government amended the [*Security of Critical Infrastructure Act 2018*](#) (SOCI) to strengthen the security posture of critical infrastructure entities. Changes to the SOCI took effect in early 2022 and include:


- increased coverage of sectors (water, gas, power, health and many others)
- mandating entities to report cyber incidents
- obligations on entities to maintain their risk management program for cyber, people, supply chain and physical security
- entities including WA public sector are obliged to report critical asset information to the Cyber and Infrastructure Security Centre.

Part 2: How to protect critical infrastructure from threats

Entities require effective risk management policies, procedures and governance to mitigate threats to their critical infrastructure. This guide is not exhaustive and highlights areas that require attention including asset management, insider threats, supply chain, and cyber and physical security risks.

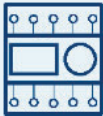
2.1 Identify and maintain an accurate inventory of important IT and OT assets

Identification and management of critical assets helps protect them against cyber and physical threats. Security of OT assets requires a different approach to IT assets.




Identify critical assets

Identify assets critical to the delivery of services. This includes sites, buildings and technology such as sensors, actuators, programmable logical controllers, servers, engineering workstations and applications.




Identify and manage asset risks

Understand the purpose of assets and relevant risks. Treat these risks with a view to minimise them as much as possible.



Get to know critical assets

Document critical asset details including their location, importance, software and firmware information and supporting vendor, where applicable. Access to this information should be granted on a need-to-know basis.



Maintain an inventory

Keep the register of critical assets current. Update it when changes are made or assets are disposed. Periodically confirm the register's accuracy.

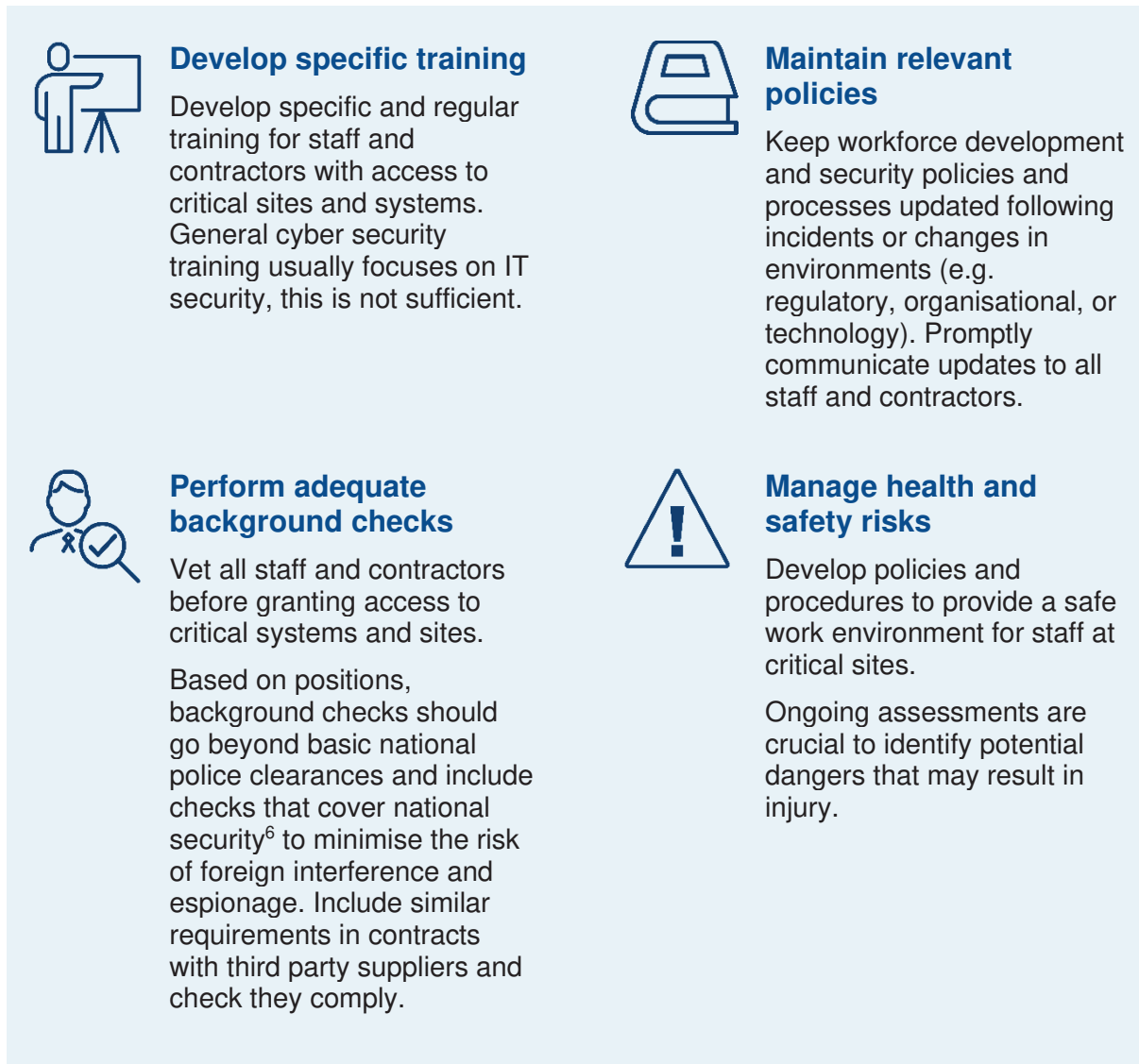
Securely dispose assets when they are no longer required or reach their end-of-life. Any information including configurations should be erased prior to disposal.

Source: OAG

Figure 3: Better practice areas for asset management

2.2 Develop a culture of security

Supporting staff through training and appropriate policies is paramount to building secure operations and a security culture. Without this, staff may not know what good security behaviours look like or how to practice them. Security programs should be tailored to roles to help develop staff understanding of risks.



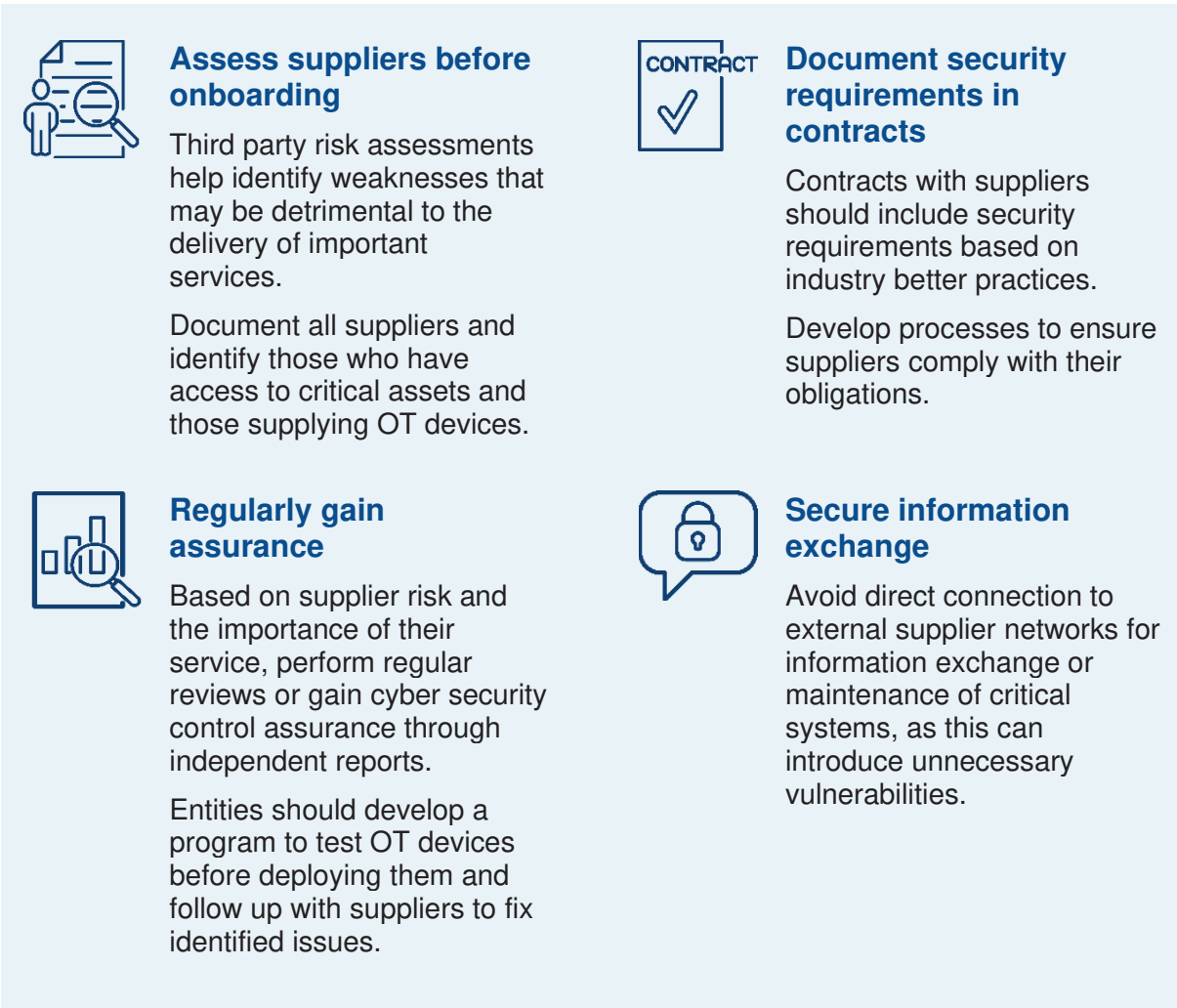
Source: OAG

Figure 4: Better practice areas for security culture

⁶ Australian Government Department of Home Affairs, '[AusCheck background checking under the Security of Critical Infrastructure Act 2018](#)', Cyber and Infrastructure Security Centre, 11 April 2023, accessed 8 June 2023.

2.3 Manage supply chain risks

Entities increasingly rely on third party suppliers to maintain their IT and OT infrastructure. It is therefore important to understand and protect against supplier risks. For example, a supply chain compromise could provide cyber criminals with an opportunity to insert malicious code in OT devices prior to delivery to entities, or while servicing or maintaining them.

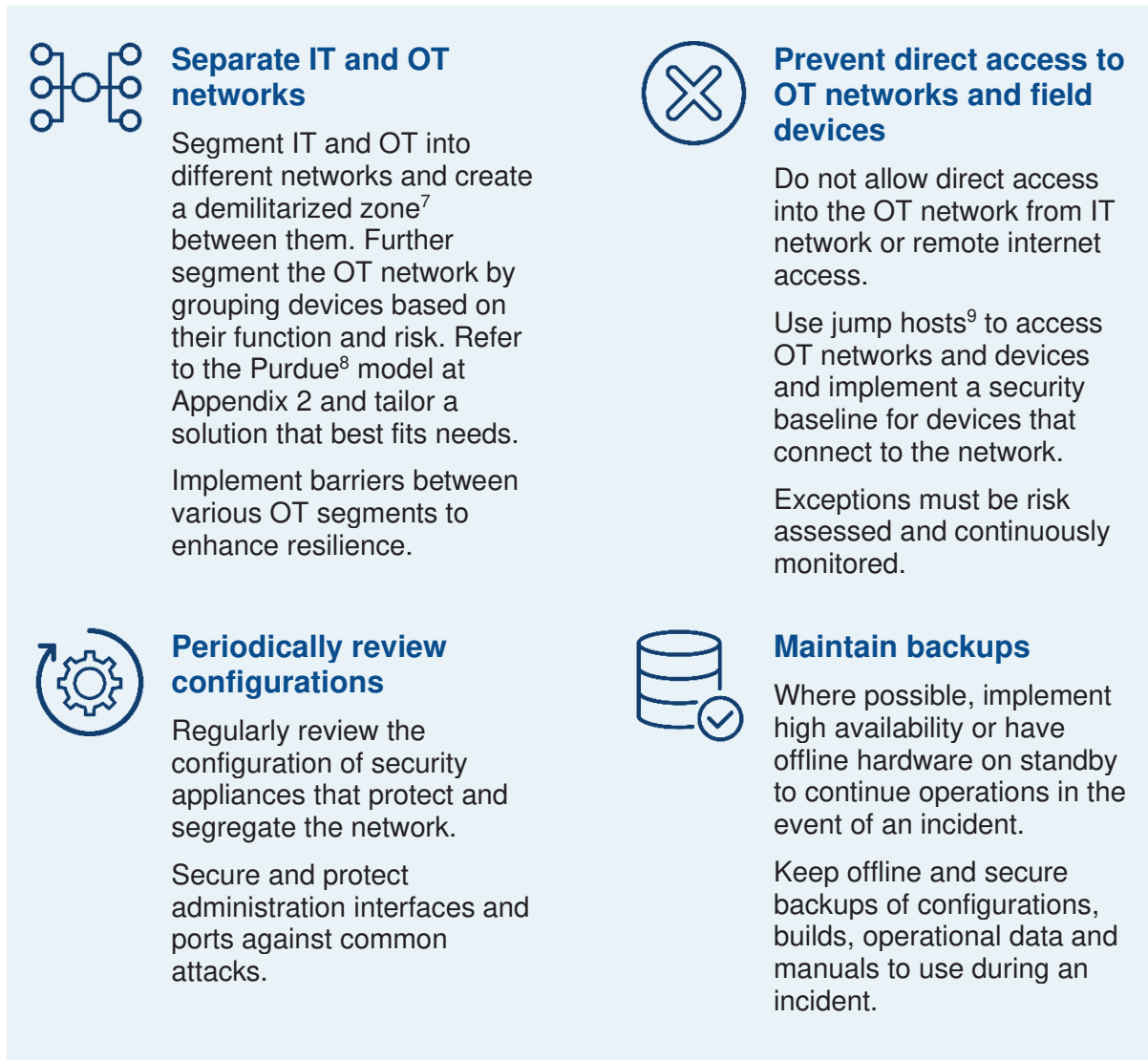


Source: OAG

Figure 5: Better practice areas for supply chain risks

2.4 Design a resilient network

Business functions often require access to the OT network or data to monitor and analyse. Careful consideration must be given to the network design needed to support business functions securely and the ongoing maintenance of network and associated devices throughout their life.



Source: OAG

Figure 6: Better practice areas for network security

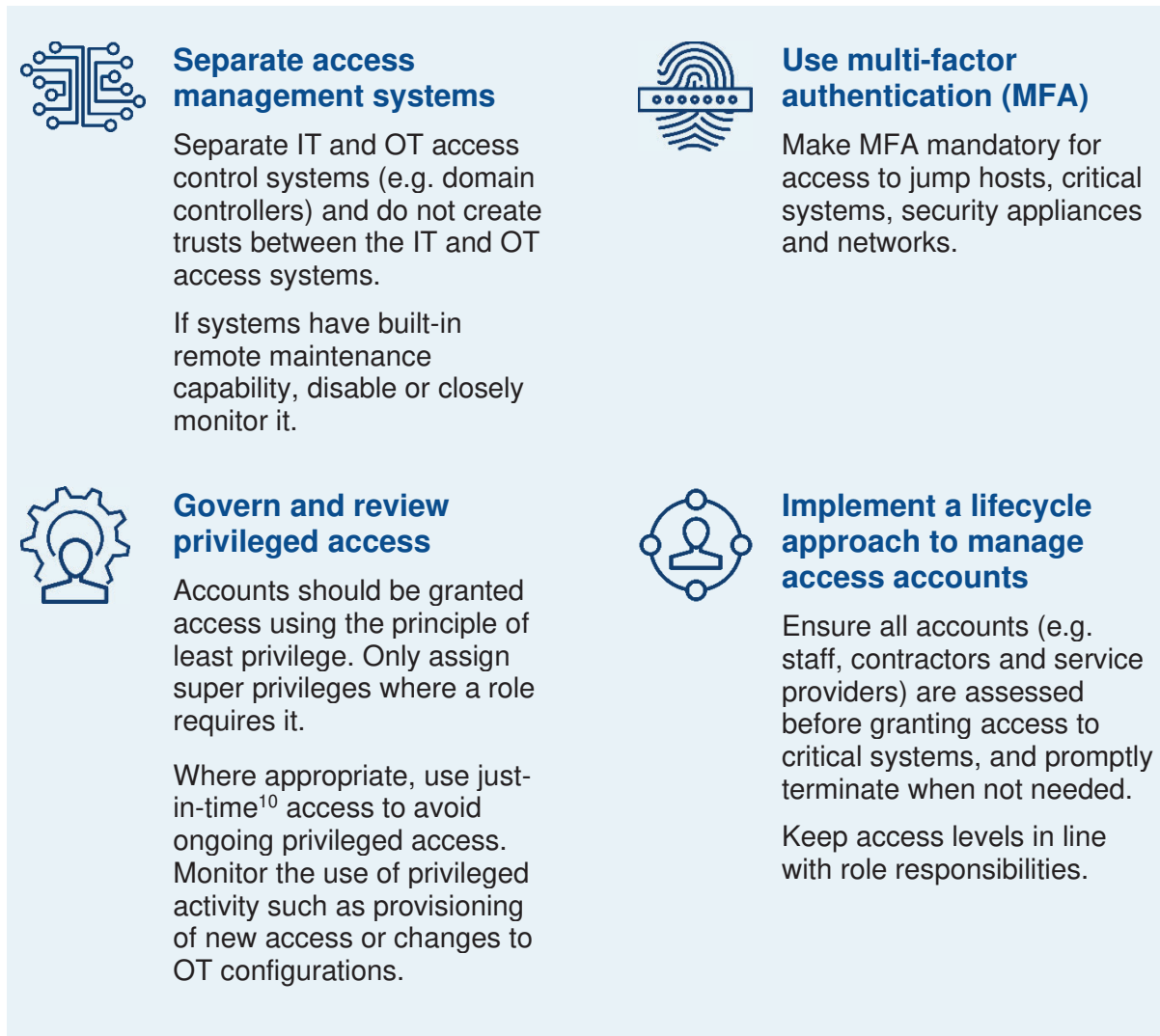
⁷ A demilitarized zone (DMZ) prevents direct access to OT assets and acts as a layer of protection.

⁸ An architecture model developed at Purdue University to manage business and industrial control networks. The model has been further expanded by various organisations to suit their needs.

⁹ A jump host is an intermediary computer used for access between two network zones.

2.5 Implement effective access management procedures

Effective access management is essential to securing IT and OT environments against cyber threats. All users and devices should be identified, authenticated and authorised before being granted access to systems and information. Unauthorised users and devices should be prevented at all levels in the network.



Source: OAG

Figure 7: Better practice areas for access management

¹⁰ Just-in-time access provides privileges for a predetermined time on a needs basis to troubleshoot, upgrade or patch applications and systems.

2.6 Manage vulnerabilities and maintain vigilance

IT and OT applications, operating system software and firmware may have weaknesses that could be exploited. Processes to harden and patch these vulnerabilities will minimise the risk of exploitation.

Monitoring to detect attempted or successful security breaches is equally important. However, collecting logs is not enough. Entities should use appropriate tools to analyse logs for malicious activity. Detecting a compromise can be difficult and requires ongoing tweaks and continuous vigilance. Entities should consider emerging technologies including artificial intelligence to further support their security monitoring processes.



Understand technical vulnerabilities

Proactive vulnerability scanning in OT networks is often difficult, however this does not mean it should not be done.

Passive scanning techniques, such as creating an offline image, can identify vulnerabilities for rectification in production environments. Risk and change management processes should be followed when patching vulnerabilities.



Maintain situational awareness

Subscribe to and read alerts issued by the [Australian Cyber Security Centre](#), which highlight cyber attacks on Australian and global critical infrastructure. These alerts often include techniques used by cyber criminals and indicators of compromise, which entities can use to review their own networks for potential malicious activity.



Monitor networks and systems

Conduct assessments to identify critical logs that must be captured for IT and OT. As a minimum, industry best practice and vendor recommended logs should be captured for internet traffic, host activity, access into OT networks and phishing attempts.

Additionally, include network traffic from low level field devices such as programmable logic controllers and remote terminal units for threat monitoring.

Use logs to create alerts based on scenarios that an adversary might use to compromise systems.



Prevent untrusted code and removeable media

Prevent execution of unapproved software, scripts, macros and other executables. Additionally, do not allow removeable media to be used on OT workstations and servers.

Where appropriate, implement application controls in IT and OT environments in line with the *Essential Eight* mitigation strategies.

Source: OAG

Figure 8: Better practice areas for vulnerability management

2.7 Implement physical security

Protecting physical sites and assets from threats is essential to entities' overall cyber security posture.



Establish perimeter protections

Limit entry points and deploy physical barriers around critical facilities such as purpose-built fences, walls and gates in metropolitan and regional locations. In addition, where appropriate, implement:

- video surveillance
- intrusion detection systems
- security guards.



Develop visitor management procedures

Effective visitor management procedures should include identification and registration. Supervised visits should be provided where access to OT and important systems is required.



Implement physical access controls

Restrict entry to sensitive areas where OT systems are located through access cards, biometric authentication or physical locks.

Do not use the same key for outer gates and rooms where OT devices are hosted. Ensure limited personal have access to master keys.



Perform ongoing site assessments

Perform ongoing security assessments on critical sites to identify deteriorations to layout, access systems, fences, lighting, alarms, signs and physical security screens.



Secure equipment during transportation

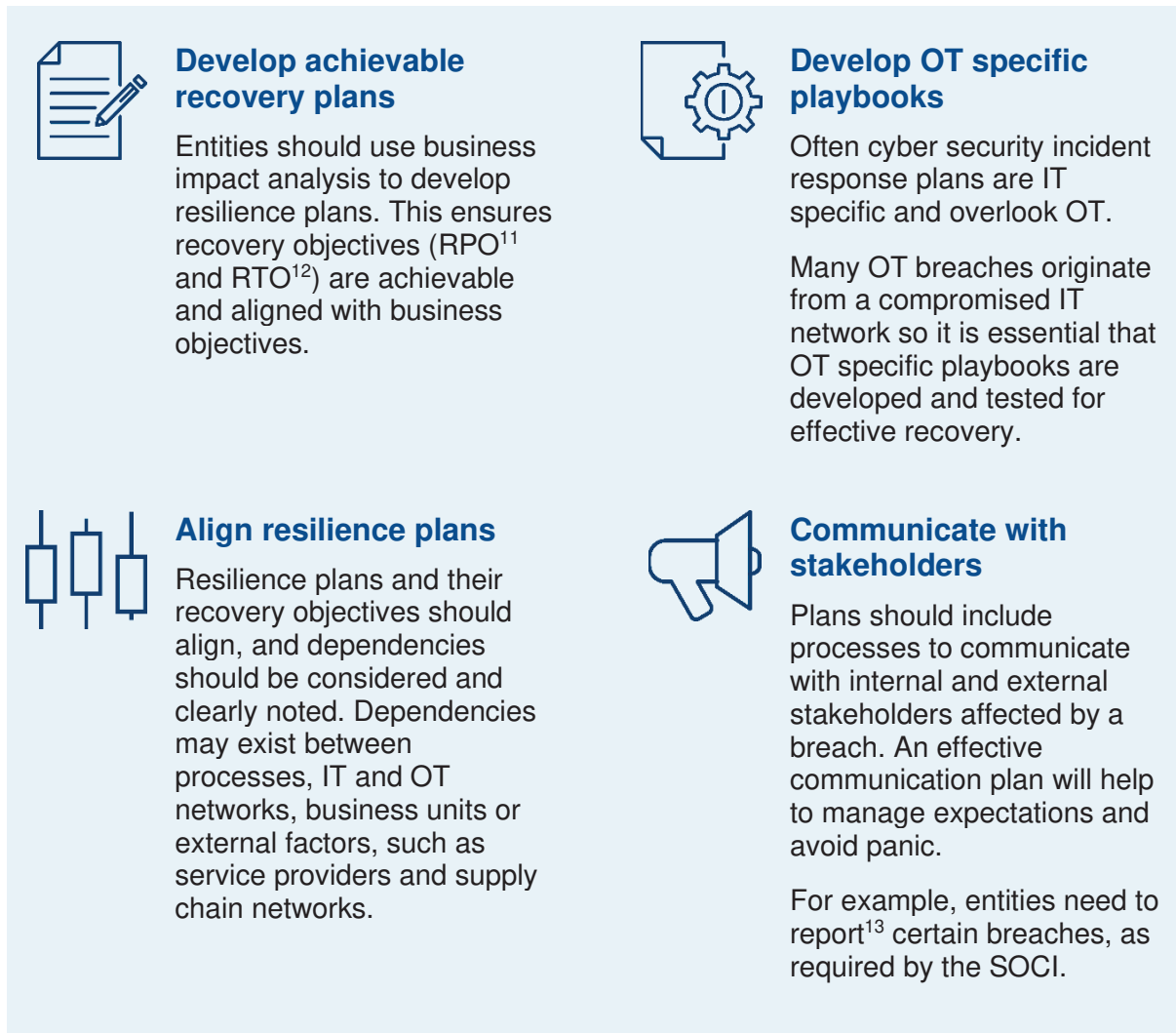
Develop procedures to minimise the risk of loss of critical assets or tampering of configuration and hardware during transportation between sites. Tamper evident seals, secure containers or trusted transportation services should be considered.

Source: OAG

Figure 9: Better practice areas for physical security

2.8 Be prepared for when things go wrong

Cyber attacks can disrupt critical systems and essential services. Entities should be prepared to manage incidents to minimise their adverse impact.



Source: OAG

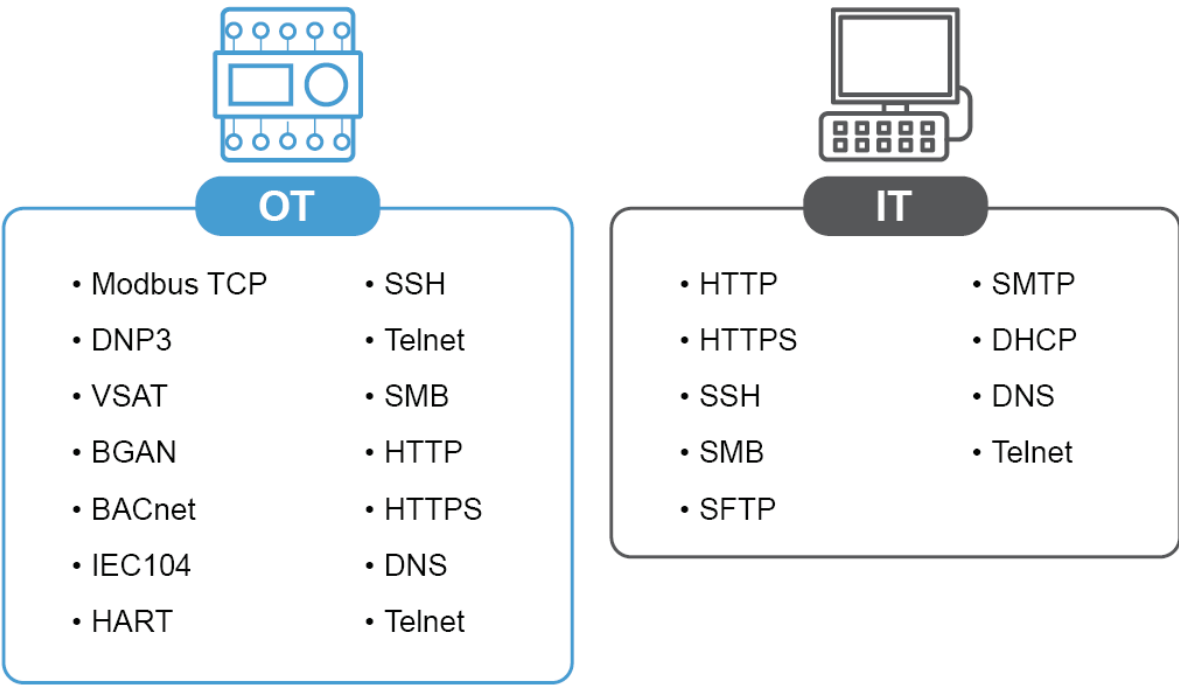
Figure 10: Better practice areas for continuity management

¹¹ RPO (Recovery Point Object) is the amount of data that will be lost or will need re-entering because of an incident.

¹² RTO (Recovery Time Object) is the amount of time that can pass before the disruption begins to seriously and unacceptably impede the delivery of critical services.

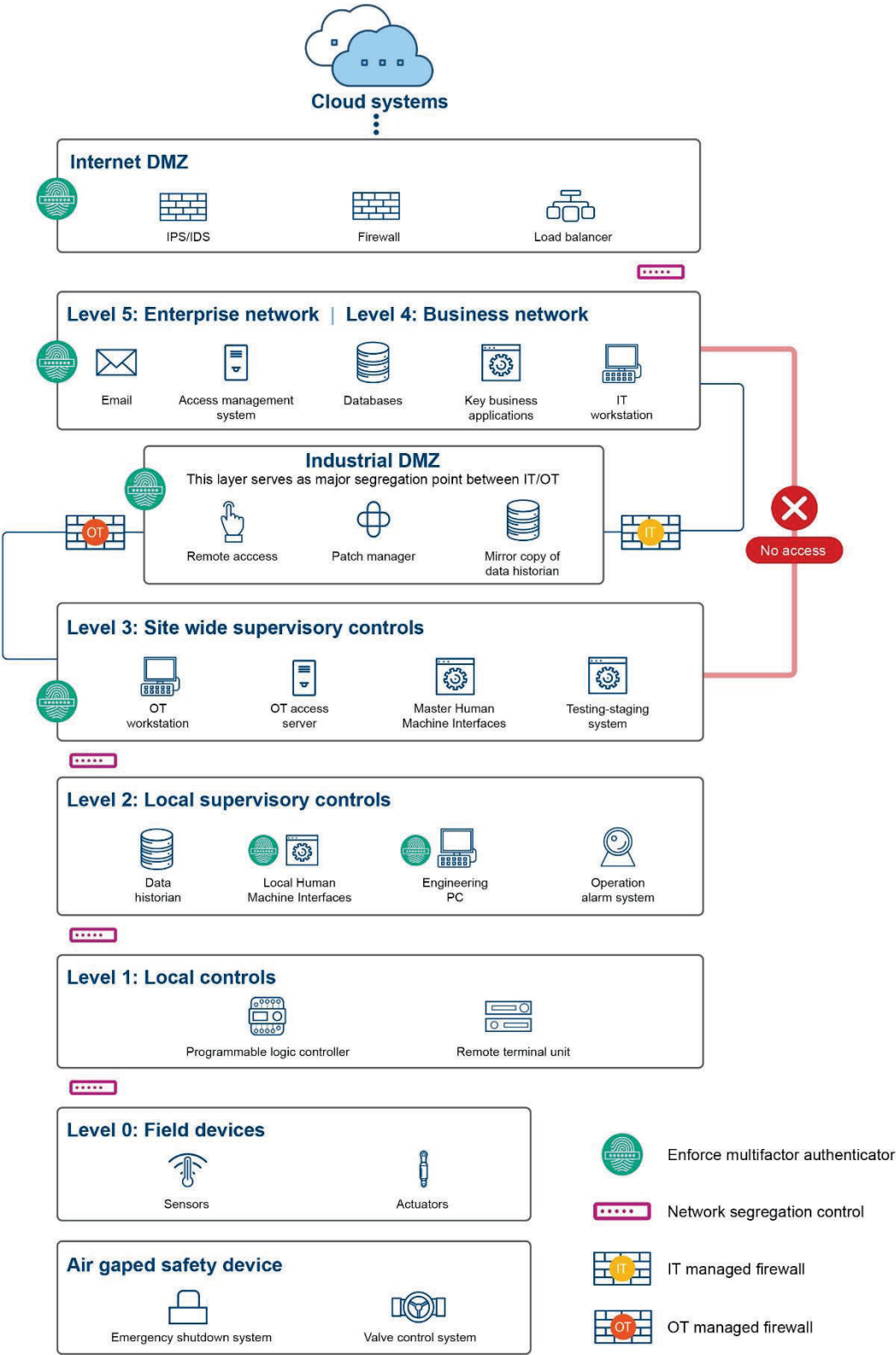
¹³ Australian Government Department of Home Affairs, [Cyber Security Incident Reporting](#), *Cyber and Infrastructure Security Centre*, 23 February 2023, accessed 8 June 2023.

Appendix 1: Examples of common OT and IT communication protocols



Source: OAG

Appendix 2: OT network segmentation – Purdue Model



Source: OAG based on the Purdue Model

Auditor General's 2022-23 reports

Number	Title	Date tabled
23	Contractor Procurement – Data Led Learnings	14 June 2023
22	Effectiveness of Public School Reviews	24 May 2023
21	Financial Audit Results – State Government 2021-22 – Part 2: COVID-19 Impacts	3 May 2023
20	Regulation of Air-handling and Water Systems	21 April 2023
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation of Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
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



Office of the Auditor General
for Western Australia



Report 26: 2022-23 | 30 June 2023

BETTER PRACTICE GUIDE

Audit Readiness



**Office of the Auditor General
Western Australia**

Report team:

Grant Robinson
Subha Gunalan
Financial Audit
Technical and Audit Support
Information Systems and Performance Audit
Forensic Audit

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.

© 2023 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: Andrey_Popov/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Audit Readiness – Better Practice Guide

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

AUDIT READINESS – BETTER PRACTICE GUIDE

This report has been prepared for submission to Parliament under sections 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 fifth comprehensive stand-alone better practice guide we have produced.

The content of this guide and recommended tools are available on www.audit.wa.gov.au and will be updated as required.

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

CAROLINE SPENCER
AUDITOR GENERAL
30 June 2023

Contents

Auditor General's overview	5
Part 1: Introduction	6
1.1 Who should use this resource	7
1.2 Using this resource.....	7
1.3 Future updates	8
1.4 Definitions	8
1.5 Limitations	9
1.6 Feedback	9
1.7 Acknowledgement	9
Part 2: Frequently asked questions	10
Part 3: Entity financial audit file requirements.....	12
3.1 Financial statements review	12
3.2 Prepared by client listing	12
3.3 Materiality.....	13
3.4 System of internal control and service organisations	15
3.5 Fraud.....	20
3.6 Going concern assessment	21
3.7 Understanding the journals process	22
3.8 Disclosure of related parties and related party transactions.....	23
3.9 Lead schedules	24
3.10 Property, plant and equipment and infrastructure fair value assessment – State government sector.....	25
3.11 Property, plant and equipment and infrastructure fair value assessment – local government sector.....	27
3.12 Impairment of assets	28
3.13 Using the work of an expert.....	34
3.14 Changes in accounting policy and estimates, and prior period errors	35
3.15 General computer controls	37

Auditor General's overview

Being audit ready is more than simply providing a draft set of financial statements and key performance indicators (KPIs) to the auditors. The essence of a good entity financial audit file is a clear trail of evidence that supports each item within the annual financial report. It means having full and complete financial statements (including relevant disclosure notes and KPIs) available for the auditors at the start of the year end audit phase. Working papers to support balances and judgements within these statements are required to be prepared *before* auditors commence, including completed reconciliations (assets/bank/leave etc.) for each month of the year. The demands and expectations of finance teams are quite significant in this regard. However, if the effort is invested in this upfront the payback will be received in a smoother and significantly more efficient audit process for all.



The record number of audit qualifications in recent years reveals there is currently a widespread need to build and improve capacity and capability within finance teams at public sector entities. This guide is one of our contributions to this cause.

In many cases, entities have an expectation that auditors will work intensely with them to resolve matters so that audits can be finalised on time. This creates additional unscheduled demands on the audit team and essentially shifts resourcing from the entity to the OAG. A sense of professional duty and service sees our auditors wanting to help, but our schedules are tight and unplanned overtime results in additional fees and auditor fatigue. Too much engagement during the financial reporting process can also impair auditor independence and risk breaching our professional standards.

Accountable authorities and chief executive officers need to ensure that their finance teams are appropriately resourced to ensure they are audit ready within agreed timeframes. We acknowledge the part we play in this also and continue to provide guidance and support where we can.

This guide caters for the many challenges and issues faced by State and local government entities and my Office, including protracted audits, inadequate audit file submissions and consequently escalating audit costs. We have also produced this content as an online resource, including video presentations and templates, that is easy to use and apply. These resources will be updated on our website from time to time. This guide is complementary to our financial statements better practice guide.

It is hoped this guide will assist entities in reducing the number of audit queries, issues, adjustments and time. Ultimately smoother and more efficient external reporting and audit processes will be better for the sector, stakeholders and the community.

Part 1: Introduction

Preparing financial statements for audit is a complex annual project requiring significant time and resources throughout the year. This guide aims to help public sector entities be ready for audit with a high-quality financial audit file and encourages continuous improvement in practices and processes for a more efficient and smoother audit for all. It complements our other better practice guide, *Western Australian Public Sector Financial Statements – Better Practice Guide*.

We acknowledge many Western Australian (WA) State and local government entities face capability and capacity issues from time to time. These issues can lead to poor financial audit file submissions, delays in finalising the audit and escalating costs. While most entities can overcome these hurdles and provide good quality, timely financial and key performance indicator (KPI) reports, supported by sufficient appropriate documentation, challenges remain for some entities.

We recognise our role in contributing to education and addressing any gaps and, where possible, to ensure public sector financial reporting and audit processes are of a high standard. However, our duty and capacity to provide hands-on support to entities is limited – our auditors must remain independent from the entities we audit. Independence is inextricably linked to an auditor's job, it is required by law as well as our professional standards. It is also expected by our community, the Parliament, lenders to our State and other stakeholders. Quality independent audit increases rigour in public administration and reporting, and enhances trust in that information and in government.

The audit readiness tool will help entities understand the audit process and prepare the entity financial audit file which contains the information we need for their financial audit. It will enable entities to have the necessary information in a manner that meets our requirements, in a useful format and with the requisite details, when we start the audit. Better preparation and being audit ready, should mean fewer queries from the financial audit teams, timely completion of the audit and potentially reduced audit costs.

State and local government entities can contribute to more effective and efficient financial audits by:

- understanding financial statement and KPI audit requirements and auditor expectations
- establishing proper review, quality assurance and sign-off of information provided to the auditors
- sticking to financial reporting timelines, including agreed financial audit timetables
- providing information to auditors in a timely and consistent manner
- advising the financial auditors of entity and accounting issues they may not be aware of
- effectively managing processes that interact with financial statement audits. These may include:
 - information systems audit typically performed by a separate team to the financial audit team
 - specialist reports (e.g. valuation reports, actuarial reports)
 - subsidiary, joint arrangement and associate audits
 - comfort letters (internal/external)
 - service organisation controls reports or equivalents
 - certifications (e.g. grant acquittals).

1.1 Who should use this resource

The primary audience of this resource is public sector financial reporting staff including chief finance officers (CFOs), chief information officers (CIOs) and those involved in setting KPIs. Chief executives (accountable authorities) can inform themselves of what is required to satisfy external reporting and assurance obligations so that appropriate resources and oversight are in place.

1.2 Using this resource

This resource is designed to give entities the tools to improve internal controls and financial processes, to help better prepare for their annual financial audit. We encourage entities to consider this tool in the context of other guidance material we may produce (for example, our better practice guides on fraud risk management, financial statements, audit committees).

The extent to which different entities refer to this audit readiness tool will vary depending on factors such as the size and classification of the entity, the experience of their finance and other teams, as well as the maturity of their financial statement processes, financial management and IT systems.

When entities are fully prepared for a financial audit, it helps us to complete the audit most efficiently and effectively. We have produced, in addition to the prepared by client listing (PBC listing), specific information requests, guidance, checklists and templates. When completed these will support the financial statements, and where relevant KPIs, submitted for audit. This is essentially a tool to help entities collate documents that the auditor needs as audit evidence. Completing this file will also help entities answer questions that your auditor, accountable authority, boards, councils and audit and risk committees may have. The information can also help the auditor understand your business better and help plan the audit.

The essence of a good entity financial audit file is a clear trail of evidence that supports each item within the annual financial report.

To help entities build this trail, we have indicated the requirements for most financial statement items. These outline the types of supporting documentation we need in order to verify each account balance in financial statements.

We have also included guidance on what some of the evidence may look like.

1.2.1 Video guidance



We have also developed brief videos that outline the entity financial audit file preparation process and how to use this resource to gain maximum benefit. These are available on our website, audit.wa.gov.au, under Resources.

1.2.2 Tools are available for download



The documents entities need to complete their financial audit file are available from our website, under Resources in Word or Excel format. Tools available on our website are identified in this report by a tool icon.

1.3 Future updates

We will continue to update this resource on our website to reflect changes in client practices and audit needs, as well as providing sector-specific supplements.

1.4 Definitions

Audit readiness tool (or resource): refers collectively to the online guidance and toolkit containing checklists, questionnaires and templates to assist entities with preparation of their financial audit file.

Better practice financial statements preparation process: is defined as structured and repeatable practices and processes that entities apply to produce clear, succinct, accurate and timely financial statements that comply with requirements and meet the needs of users.¹

Underlying better practice financial statement preparation is an effective risk management and internal control framework. Entities should refer to our *Western Australian Public Sector Financial Statements – Better Practice Guide* for principles in designing, implementing and maintaining (or using) a system of internal control over external financial reporting that supports the preparation of financial statements.

Certifications: refers to the audit or acquittal of financial statements or financial information required under Commonwealth and State grant and other funding agreements and commitments, for example Royalties for Regions and Roads to Recovery.

Entity financial audit file: refers to the electronic file that the entity's staff will prepare which contains the financials auditor's information requests and supporting documents for the financial audit.

Financial audit: refers to the audit of financial statements and KPIs (as applicable). The terms external audit and financial audit are used interchangeably throughout this resource. The audit will include an examination of the underlying internal control framework that supports the preparation of financial statements and KPIs.

Financial audit team: includes OAG financial audit staff and staff of firms contracted by the OAG.

Financial statements and financial reports: these terms are used interchangeably.

For State government entities:

Relates to financial statements prepared under the *Financial Management Act 2006* (FMA), enabling legislation of non-FMA entities, and includes the Annual Report on State Finances prepared under the *Government Financial Responsibility Act 2000*.

For local governments entities:

Relates to annual financial reports prepared under the *Local Government Act 1995* (LG Act) and Local Government (Financial Management) Regulations 1996.

Independent Auditor's Report: for State government entities, the Auditor General's report on the audit of the financial statements includes an opinion on the financial statements, KPIs and controls; and for local government entities, this includes an opinion on the financial statements.

Key performance indicators (KPIs): for State government entities, KPIs provide an overview of the critical or material aspects of outcome achievement and service delivery.

¹ Office of the Auditor General, *Western Australian Public Sector Financial Statements – Better Practice Guide*, OAG, Perth, 2021, p. 12.

1.5 Limitations

The purpose of this resource is to encourage better practices for financial audit readiness. The information is general in nature and subject to change if an audit warrants. It does not cover every eventuality or all the information the audit team may need.

The resource is not intended to be a definitive point of reference for the audit requirements of specific entities. Each entity should ensure its own familiarity with the relevant audit requirements based on their respective financial statements and unique accounting issues, in discussion with their audit team.

We recommend users exercise their own skill and care with respect to their use of this resource and that users carefully evaluate the accuracy, currency, completeness and relevance of the material for their purposes.

1.6 Feedback

We welcome entities to provide feedback and suggestions to info@audit.wa.gov.au on how they find using the resource and what else they would find useful.

1.7 Acknowledgement

While we have developed content that is specific to and tailored for the Western Australian context, we would like to acknowledge in general that the content, including video transcripts, specific information requests, templates, checklists and questionnaires have been largely drawn from an Audit New Zealand resource² with permission from Audit New Zealand.

We would like to thank Audit New Zealand and stakeholders with whom we consulted to tailor this resource.

² Audit New Zealand, [Client Substantiation File](#), Audit NZ website, 2020, accessed 30 March 2023.

Part 2: Frequently asked questions

We receive many queries from entity staff on various aspects of the financial audit process. This section answers some of the common questions we receive and clarifies the roles and responsibilities of entity staff and the financial auditor.

1. Why do auditors ask the same question and request the same information every year?

Financial reporting and audits are an annual process. Auditing standards generally require fresh assessment of an entity's information and systems of internal control to be undertaken annually. Therefore, the same or similar questions may be repeated every year. Fresh assessments are required to identify the risk of material misstatements as it forces the information to be considered independently and objectively without bias and other influences. Examples of annual assessments include:

- impairment
- fraud
- going concern
- an understanding of key systems and processes.

2. What influences the cost of an audit?

There are various factors that affect audit costs. Generally, audit costs increase annually due to such factors as market forces, Consumer Price Index (CPI) increases, changes in accounting or auditing standards, regulatory changes, changes in underlying operations (e.g. new service lines) or machinery of government changes. Our experience, however, is that significant fee increases in recent years have arisen from entities not being audit ready – hence the development of this resource. We want to help make the audit process as smooth and efficient as possible for all of us.

3. Why is there a need to assess property, plant and equipment, and infrastructure balances yearly if there are no material movements?

Financial reporting frameworks for public sector entities requires compliance with Australian Accounting Standards (AAS) and relevant laws and regulations. Many public sector entities are required to apply the revaluation model (fair value) for certain classes of property, plant and equipment (PPE), and infrastructure under AAS. Under the revaluation model, entities are required to ensure that the relevant PPE and infrastructure asset balances materially represent fair value at each reporting date.

Management should undertake an assessment each year to determine whether there has been a material movement or not in the fair value of the relevant asset classes. Management should document their assessment of the current market conditions and any other relevant factors that may impact on the fair value of the asset balances. Without undertaking such an assessment each year, it would be difficult to convince an auditor that there has not been a material movement in the asset balance for the year.

4. Why are different auditors coming each time with limited experience in the sector or in auditing as a whole?

Audit teams generally comprise different levels of staff, including graduates who are new to the sector and the audit process. Training quality graduates both on the job and through advanced qualifications (CPA, CA) is something the audit profession has long prided itself in.

Our graduates provide a pipeline of not just great future auditors, but highly qualified finance professionals for the community.

All audit staff (including those of our contract audit firms) are assigned appropriate tasks based on their experience and training, with ongoing supervision and review of their work. So as to avoid any inefficiencies arising out of lack of knowledge or training, we run regular training for our staff (including those of our contract audit firms) on technical updates on accounting/auditing standard changes, other regulatory updates, as well as inviting external presenters to cover topics relevant to increasing our knowledge of the public sector and the issues being audited (including importantly local government).

5. What is the impact on the audit process when there is a new auditor and a new in-house accountant?

The audit process remains the same, regardless of changes in personnel. From an audit perspective, continuity of staff is always considered when allocating staff to audits. However, from time to time new staff are rotated in to maintain auditor independence and objectivity. To reduce inefficiencies, we encourage new entity staff to engage with the auditors early to understand requirements and the audit process.

Part 3: Entity financial audit file requirements

3.1 Financial statements review

The accountable authority, council, chief executive officer (CEO) and the chief finance officer (or equivalent) are ultimately responsible for the integrity of financial and performance reporting within the entity. By providing a signed declaration on the financial statements and KPIs (as applicable), it confirms their responsibility to ensure adequate processes and controls exist to support the preparation of the financial statements and a report on KPIs (as applicable). A change to the audit process has been implemented whereby a certified set of financial statements and a report of KPIs should be submitted to the auditors at the commencement of the final audit stage. The certification is the standard certification management normally use in the audit process. The change is to re-emphasise the responsibilities of the accountable authority, council, CEO and chief finance officer (or equivalent).

The audit committee assists the accountable authority/council by providing a second level of assurance through the review of the financial statements and KPIs (as applicable) and giving its independent view and recommendations. It is a natural role of the audit committee to review the financial statements and KPIs (as applicable) to determine whether they reflect the audit committee's understanding and provide a true and fair view of the financial position and performance of the entity. This will include whether management has exercised appropriate accounting judgements and considerations in preparing the financial statements and KPIs (as applicable). Records of the audit committee review comments and recommendations will be evident in minutes of meetings as part of the audit committee meeting process. The audit committee is not expected to sign the financial statements and KPIs (as applicable).



The financial statements checklists, available from our website, are a useful tool for the finance team in ensuring quality of the financial statements and should be completed prior to presenting the financial statements to the financial audit team for audit.

Guidance material for the audit committee is available in the *Western Australian Public Sector Audit Committees – Better Practice Guide*³.

3.2 Prepared by client listing

Our audit of entities is split into two components spread over one or more visits: interim audit and final audit.

The interim audit includes:

- preliminary planning and detailed planning
- updating our understanding of the entity's business
- updating our understanding of the control environment and assessing the design and implementation of key controls and, where appropriate, whether they are operating effectively
- relevant activities pertaining to the general computer controls (GCC) audit

³ Office of the Auditor General, *Western Australian Public Sector Audit Committees – Better Practice Guide*, OAG, Perth, 2020.

- sample testing of transactions to confirm the accuracy and completeness of processed accounting transactions clarifying significant accounting issues before the annual financial report is prepared for audit
- reviewing legislative compliance (applicable State and local government financial and other relevant legislation and the compliance culture of the entity)
- reviewing proposed KPIs (if applicable) for relevance and appropriateness
- follow-up of prior year findings and conduct preliminary analytical review.

The final audit focuses on verifying the financial statements, notes and KPIs (where applicable) and includes:

- understanding the controls over financial statement preparation
- verifying high risk and material account balances using a combination of substantive analytical procedures, tests of details substantiation to subsidiary records and confirmation with external parties
- verifying KPIs (where applicable)
- reviewing the annual financial report and notes for compliance with the *Financial Management Act 2006*, the Treasurer's instructions, *Local Government Act 1995*, Local Government (Financial Management) Regulations 1996, as applicable, and the AAS.

We discuss our requirements with entity staff to facilitate a timely, efficient and effective audit. We formally agree our information requirements and timeframes for the final audit with the entity's chief finance officer using our PBC listing. This PBC listing is intended to help staff have various documents readily available when we perform our audit. However, in several instances, particularly during audit sampling at the interim visits, financial auditors will need to retrieve some evidence themselves, rather than being given the evidence by entity staff. This is essential for an independent audit.



Sample PBC listings for the interim and final phases which will be tailored to the entity are available on our website.

3.3 Materiality

Materiality is both an accounting and auditing concept. From an accounting perspective, materiality is an overriding concept that applies to the preparation and presentation of financial statements, in addition to the applicability of the AAS requirements:

Information is material if omitting, misstating or obscuring it could reasonably be expected to influence decisions that the primary users of general purpose financial statements make on the basis of those financial statements, which provide financial information about a specific reporting entity (AASB 101.7).

Materiality possesses both quantitative and qualitative factors, with the latter requiring more judgement. Some useful guidance is contained in AASB 101 *Presentation of Financial Statements* and in AASB Practice Statement 2 *Making Materiality Judgements*. AASB Practice Statement 2 articulates a four-step materiality process that entities may apply in assessing materiality in preparing their financial statements. A good diagram of the four-step process is available in the AASB Practice Statement 2 (paragraph 34, page 16).

The entity needs to assess how users of financial statements (with a reasonable knowledge of business and economic activities) could reasonably be expected to be influenced in making economic decisions (AASB 101.7).

Finally, AASB 108.8 highlights the need to balance AAS requirements with materiality assessments. While it is appropriate to not apply some accounting policies where the effect is immaterial, 'it is inappropriate to make, or leave uncorrected, immaterial departures from the AAS to achieve a particular presentation of an entity's financial position, financial performance or cash flows'.

Note that certain requirements under legislation, policy instruments or other authoritative requirements are to be strictly complied with, except where the requirement permits the materiality concept to be applied.

3.3.1 Assessing materiality

Both the entity and OAG have a responsibility to consider and apply materiality in the context of the accounting and auditing standards respectively. It is therefore important that an entity's approach to materiality considers the OAG's approach with the aim of ensuring as far as possible, that both approaches are compatible. It is also important to note that entity's management cannot set or influence materiality for the financial statements audit.

While materiality is a pervasive concept and requires judgement, entities are to follow the financial reporting requirements, including the application of accounting policies, set by the respective regulators, namely the Department of Treasury (Treasury) for State government entities and the Department of Local Government, Sport and Cultural Industries (DLGSC) for local government entities. For consistency and compliance, entities may find it useful to follow the relevant model financial report issued by Treasury and DLGSC, including the appropriate accounting policies and disclosure, and presentation of the financial statement and notes.

It is not appropriate for an entity to make, or leave uncorrected, immaterial departures from AAS requirements to achieve a particular presentation in the financial statements, or to clutter the financial statements with immaterial information that distracts the reader from the material information.

Entities as a minimum should comply with the prevailing legislative reporting framework (FMA, Treasurer's instructions, LG Act etc.) and meet the requirements of the AAS. Entities are to apply their materiality in respect of identifying and correcting errors and misstatements in their financial statement preparation process. It would not be appropriate for an entity to rely on purely numerical guidelines or to apply a uniform quantitative threshold for materiality.

The auditor materiality is different to management materiality. The concept of auditor materiality applies in planning and performing the audit, in evaluating the effect of misstatements including any uncorrected misstatements on the financial report and in forming the auditor's report. Auditors consider materiality together with audit risk, a representation of the risk of material misstatements and detection risk. The identification and assessment of risk of material misstatements involve the use of auditors' professional judgement. Disclosures in the financial report are also assessed for qualitative misstatements (i.e. in general, misstatements are considered to be material if they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial report as a whole).

It is important to note that while the concept of materiality and its application results in efficiencies, better practice entities will promote an environment in which the correction of errors and misstatements, including fraud and addressing internal control deficiencies, is seen as the appropriate course of action, as long as this is cost beneficial.

3.4 System of internal control and service organisations

3.4.1 Why is the auditor required to understand the components of the entity's system of internal control?

The system of internal control consists of:

- the control environment
- the entity's risk assessment process
- the entity's process to monitor the system of internal control
- information systems and communication
- control activities.

Financial auditors consider these five inter-related elements individually and collectively to understand an entity's system of internal control.

The auditor's understanding of each of the components of the entity's system of internal control provides insight into how the entity identifies and responds to business risks. Evaluating the effectiveness of control design and their implementation may also influence the auditor's identification and assessment of the risks of material misstatement in different ways. This assists the auditor in designing and performing further audit procedures, including any plans to test the operating effectiveness of controls. For example:

- The auditor's understanding of the entity's control environment, the entity's risk assessment process, and the entity's process to monitor control components are more likely to affect the identification and assessment of risks of material misstatement at the financial report level.
- The auditor's understanding of the entity's information systems and communication, and the entity's control activities component, are more likely to affect the identification and assessment of risks of material misstatement at the assertion level (ASA 315).

Risks of material misstatement affect the auditor's design of overall responses, including, an influence on the nature, timing and extent of the auditor's further procedures (ASA 315).

3.4.2 Control environment

The control environment provides the foundation for the system of internal control. It does not directly prevent, or detect and correct, misstatements. It may, however, influence the effectiveness of controls within the control system. Similarly, the entity's processes for assessing risk and monitoring the internal control system are designed to operate in a manner that also supports the entire system of internal control (ASA 315).

The control environment reflects the overall attitudes, awareness, and actions of management, the governing body, owners, and others concerning the importance of control and the emphasis given to control in the entity's policies, procedures, methods and organisational structure. The control environment encompasses:

- the development of accounting and KPI estimates
- the external reporting philosophy
- the context in which the accounting system and control procedures operate.

The control environment sets the tone of an entity, influencing the control consciousness of its people. Some best practice examples include establishing, communicating and updating codes of

conduct, establishing effective audit committees that oversee financial reporting and clearly defining roles, responsibilities and delegation of authority.

Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial report and KPIs.

3.4.3 Risk assessment process

The entity's risk assessment process forms the basis for how management and the governing body determine the risks to be managed. If that process is appropriate to the circumstances, including the nature, size and complexity of the entity, it assists the financial auditor in identifying risks of material misstatement. Whether the entity's risk assessment process is appropriate to the circumstances is a matter of judgement. Generally, financial reporting items that are subject to judgement such as accounting estimates, for example, fair values of infrastructure assets, provision for employee entitlements, would be an area of focus for the auditors.

An auditor's risk assessment will also include fraud risk and auditors may undertake journal entries testing among other procedures to assess the risk.

3.4.4 Process to monitor system of internal controls

Monitoring of controls relates to management's ongoing review of the effectiveness of control, identification and remediation of control deficiencies that are relevant to financial reporting, including the process of an internal audit function. Monitoring is done to ensure that controls continue to operate effectively over time. For example:

- management monitoring of controls to determine their effectiveness
- regular reporting of status of audit deficiencies and corrective action taken to audit committee
- separate evaluations conducted periodically, such as internal audits
- a combination of internal audits and reporting to audit committee.

3.4.5 Information systems and communication

Information systems relevant to the preparation of the financial report consist of activities and policies, accounting and supporting records, and various business processes established to support financial reporting.

Entities should maintain data flow diagrams, flowcharts, descriptions and procedure manuals that support internal control and financial reporting. These documents are produced so that information about these processes can be easily understood by users throughout the entity, including the IT team, finance and accounting specialists, system developers, support staff and auditors. This documentation allows staff and other users to identify the source of data, responsible staff, storage locations, source documents, relevant transformation processes, quality checks and the primary users.

Communication refers to roles and responsibilities of individuals relating to the system of internal controls and financial reporting. This can take the form of policies and manuals, exception reporting and evaluation, or oral communication of significant financial reporting matters.

Entities should document internal control responsibilities including who is assigned to perform, review and assess individual internal controls. This documentation should be accessible to management and staff responsible for external financial reporting.

Entities should review external audit findings, such as OAG management letters, and identify any internal control issues or recommendations, assign an appropriate staff member to formally respond to these matters and communicate to senior management and audit committee the proposed resolution.

3.4.6 Control activities

Control activities are those policies and procedures established and applied by management that enable proper accounting and recording. They encompass controls over significant risks, key business cycles, journal entries and IT applications.

Control activities can be preventative or detective and include activities such as delegations, authorisations, reconciliations, segregation of duties, physical security of assets, systems access and security. These are important controls that individually or in combination with others, can help prevent, detect and correct misstatements in classes of transactions, account balances or note disclosures.

Entities should design and implement key controls to address financial reporting risks adequately. Key controls must be designed and implemented to prevent or detect potential material misstatements related to the identified financial statement assertions in a timely manner.

For all controls, establish a standard of what initiators and reviewers must do and how to evidence that they have performed the control or review (for example sign-offs, reconciliations and ensuring documentation is properly retained). This requires staff training and supervision.

Better practice entities have financial management information systems capable of producing complete, accurate and reliable information. It is also important that system functionality supports processing and information requirements for the financial statements. For example, configure the IT infrastructure to support restricted access and segregation of duties.

Based on the auditor's evaluation of each of the components of the entity's system of internal control, the auditor will usually determine whether one or more control deficiencies have been identified and report it to management and those charged with governance.

3.4.7 Service organisations

Entities should obtain assurance reports (service organisation controls 'SOC' reports or equivalent) when they use third party vendors to provide cloud applications for key systems including payroll and finance. These reports provide assurance that the vendor is following good practices and maintaining an effective control environment. Assurance reports are prepared by independent auditors and provide comfort that appropriate controls are in place to protect the confidentiality, privacy, integrity and availability of data. In particular, they provide insights on risks that may need to be considered when contracting services to third-party vendors and ongoing management during the contract.

There are two types of service organisation controls report:

- Type 1 provides assurance on the design and implementation of controls by the third-party vendor. While it provides information on controls, it does not provide assurance that these controls were operating effectively. Therefore, it is not suitable for financial audit requirements.
- Type 2 provides assurance on whether the controls operated by the third-party vendor are designed and implemented appropriately and are operating effectively during the period. Only this type of report is suitable for financial audit requirements.

3.4.8 What do auditors specifically focus on when understanding a system of internal control?

When understanding and assessing the system of internal control, the financial auditor focuses on the different activities performed for processing data (both financial and non-financial, where relevant).

Controls relating to systematic processing and handling of data fall within the following categories:

- policies and procedures – are appropriate and support reliable processing of information
- security of sensitive information – controls exist to ensure integrity, confidentiality and availability of information at all times
- data input – information entered is accurate, complete and authorised
- backup and recovery – is appropriate and in place in the event of a disaster
- data output – online or hard copy reports are accurate and complete
- data processing – information is processed as intended, in an acceptable time
- segregation of duties – no staff perform, or can perform, incompatible duties
- audit trail – controls over transaction logs ensure history is accurate and complete
- master file maintenance, interface controls, data preparation – controls over data preparation, collection and processing of source documents ensure information is accurate, complete and timely before the data reaches the application.

The processing procedures relevant to the financial auditor in understanding the flow of transactions or events, are those activities required to initiate, process and record any significant type of transaction or event. These include the procedures for correcting and reprocessing previously rejected transactions or events and for correcting erroneous transactions or events through adjusting entries. For example, in understanding an expenditure/accounts payable process, an auditor wishes to understand what initiates the process (usually the raising of a purchase order) through to the payment to the supplier and reconciliations to the general ledger. This further enables the auditor to understand and assess the process for updating the supplier's master file.

The understanding by the financial auditor will be at a level that allows them to identify whether effective internal controls are in place to ensure data is processed, recorded, presented and disclosed correctly.

The transaction processes that the financial auditor will assess are usually processes that have high volume transactions. Some common processes are:

- revenue/accounts receivables
- purchases/accounts payables
- payroll/employee entitlements
- property, plant and equipment (additions, disposals, depreciation etc.)
- cost allocation
- journals
- non-financial measures, such as achievement of KPIs.

When identifying internal controls, the financial auditor assesses whether internal controls are in place to reduce the risk of a material misstatement arising from the recognition, measurement, presentation and disclosure of various balances in the financial statements, their related disclosures and performance measures.

To assist with this, the financial auditor uses the concept of assertions, that is, when representing that the financial statements are in accordance with the applicable financial reporting framework, an entity implicitly or explicitly makes assertions regarding the recognition, measurement, presentation and disclosure of the various elements of financial statements, related disclosures and KPI information.

The assertions for financial and non-financial data are shown below:

Account assertion	Internal controls should be in place to ensure
Occurrence	Financial and KPI transactions and events that have been recorded or disclosed have occurred and relate to the entity.
Completeness	All financial and KPI transactions and events that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
Accuracy	Amounts and other data in the financial and KPI transactions and events have been recorded correctly and related disclosures have been appropriately measured and described.
Cut-off	Financial and KPI transactions and events have been recorded in the correct accounting period.
Classification	Financial and KPI transactions and events have been recorded in the proper accounts.
Presentation	Financial and KPI transactions and events are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

Source: OAG based on ASA 315

Table 1: Assertions about classes of transactions, related disclosures, and KPI results

Account assertion	Internal controls should be in place to ensure
Completeness	All assets, liabilities and equity components that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
Existence	Assets, liabilities and equity components exist.
Rights and obligations	The entity holds or controls the rights to assets and liabilities that are obligations of the entity.
Accuracy	Assets, liabilities, and equity components have been included in the financial statements at appropriate amounts and related disclosures have been appropriately measured and described.
Valuation and allocation	Any resulting valuation or allocation adjustments on assets, liabilities and equity components have been appropriately recorded.
Classification	Assets, liabilities and equity components have been recorded in the proper accounts.
Presentation	Assets, liabilities and equity components are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

Source: OAG based on ASA 315

Table 2: Assertions about account balances and related disclosures at the period end

The assertions described in the tables above, adapted as appropriate, may also be used when including any additional disclosures that are not directly related to recorded classes of transactions, events or account balances. For example, financial instrument risk and related party and key management personnel disclosures.

3.4.9 How does the financial auditor do this?

Understanding the flow of transactions, or events, is acquired by a combination of:

- asking appropriate staff at the entity
- observing the processing methods and procedures used
- reviewing the entity's manuals and other written instructions
- walk throughs, that is tracing transactions through the relevant system.

At the conclusion of this exercise, the financial auditor concludes whether there are internal controls in place that are designed appropriately and will either prevent or detect a material error with respect to the various assertion risks described above.

3.5 Fraud

The auditors are responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error.

It is important to note that a financial audit:

- does not guarantee that every amount and disclosure in the financial statements and KPIs is error free of misstatement
- does not examine all evidence and every transaction.

The accountable authority, boards, councils and senior management have responsibility for maintaining internal controls that prevent or detect fraud or error and to ensure regulatory compliance. The audit committee and the Auditor General should be informed by management of any fraud or material errors. During the financial audit, the auditors will consider management programs and controls intended to deter and detect fraud and make appropriate inquiries. It should be noted that an audit is not designed to detect fraud, however, should instances of suspected fraud come to an auditor's attention, they will report them to the entity. Information relating to the suspected fraud will be provided to the Office of the Auditor General's forensic business unit and they may decide to conduct further investigation or refer to integrity entities as appropriate.

The distinguishing factor between fraud and error is that fraud is an intentional act designed to deceive, whereas error is something that occurs by a mistake, oversight or misinterpretation of facts.

An auditor is concerned with fraud or error, particularly, that may cause a material misstatement in the financial statements. The two major types of intentional misstatements affecting the audit are those resulting from:

- Fraudulent financial reporting through falsifying records, creating false transactions or intentional misapplication of accounting policies. The primary motivation being to show performance as being better than it is.
- Misappropriation of assets by an employee (or a member of the governing body or management). The primary motivation being for personal gain.

Both types of fraud involve overriding existing controls and creating false transactions or accounting entries as part of an intentional process to prevent the fraud from being discovered.

When performing the risk assessment, it is necessary for the auditor to make enquiries within the entity of any knowledge and details around fraud that may have taken place and any suspected or alleged fraud. The enquiries will also focus on the systems in place to prevent and identify fraud.



The specific enquiries focus on management, internal audit and those charged with governance and there is a questionnaire to be completed for each. The questionnaires can form the basis for discussions at various meetings with the auditors and are helpful in understanding the operating environment and if there are any risks for the auditors to consider.

3.6 Going concern assessment

The going concern assumption is that the entity will continue to operate /remain in business (in other words, continue as a going concern) into the foreseeable future. There are requirements in AAS for management to assess the validity of the going concern assumption, looking forward at least 12 months. There are also requirements to make disclosures in the financial statements.

For State government entities the going concern risk is currently considered low. For local government entities, this risk is also considered to be generally low. However, if going concern indicators exist such as cut back of services and programs and a deteriorating financial position, a more detailed going concern assessment will be required, including relevant commentary in the notes to the financial statements. Regardless, Australian Auditing Standards require auditors to evaluate management's assessment annually. Management's assessment of the entity's going concern should include an explanation of the rationale in support of their assessment, even if management is comfortable that the entity is a going concern. For most public sector entities, management's assessment and the auditor's evaluation of it may be relatively straightforward, given the low likelihood of indicators being present that threaten the going concern assumption.

3.6.1 Responsibilities of management

When preparing financial statements, an assessment of the entity's ability to continue as a going concern must be made. Management's assessment involves making a judgement, at a particular point in time, about inherently uncertain future outcomes of events or conditions.

Where the going concern assumption is considered appropriate by management, the financial statements are required to be prepared on a going concern basis. If there is uncertainty regarding the ability of your entity to continue as a going concern, then disclosure around this will need to be included in the financial statements.

The financial statements are not to be prepared on a going concern basis when the entity has an intention to liquidate or to cease its operations, or if it has no realistic alternative but to do so.

Management should consider the following when providing their assessment and supporting information to the auditors:

- appropriation budgets and any other evidence of continued government funding commitments

- 12-month cashflow projections and forecasts
- corporate business plans including long term financial plans.

3.6.2 Responsibilities of the auditor

The Australian Auditing Standards place certain requirements on auditors relating to the application of the going concern assumption. The auditor's responsibilities in this regard are to:

- evaluate the assessment prepared by management
- obtain sufficient appropriate audit evidence about the appropriateness of management's use of the going concern basis of accounting in the preparation and presentation of the financial statements
- conclude on whether there is a material uncertainty about the entity's ability to continue as a going concern.

The auditor is required to ensure that the period of the going concern assessment is at least 12 months in the future from the date of the audit report.

The auditor will also require a written representation from those charged with governance at the end of the audit on whether or not the use of the going concern assumption is appropriate. This will normally be included in the representation letter.



The entity is required to complete an information request and return to the auditor.

3.7 Understanding the journals process

Journals are used to capture transactions into an accounting system in different ways and may often have different characteristics. Journals can be:

- used to record transactions into the accounting records
- used to correct errors of previous entries
- routine and used for transactions that occur regularly
- non-routine as they are used to capture less frequently encountered transactions.

Journals by nature have higher risk associated with them as inappropriate journals can be posted to the accounting system. It is important that there are robust processes and controls around the processing of journals. These must cover who can initiate and approve journal entries. Incorrect or inappropriate journals can be used to manipulate the accounting records and will result in errors being present in the financial statements.

It is important that the financial auditor gets a sufficient understanding of the process over journals. A proper understanding will also allow the financial auditor to identify any risk areas in the journals process and which journals to focus their audit procedures on.

It is also important that the financial auditor receives a complete list of all journals processed for the reporting year. Generally, a complete transaction listing is required, including a full journal listing in an electronic format (Excel format preferred), suitable for data analytics purposes.



A journals questionnaire is available online for entities to complete in order for their financial auditor to better understand their journals process and the risks associated with it. It will help the financial auditor to focus their attention on which journals to test. The questionnaire may also give the entity an indication of any areas in their journal process that needs attention.

3.8 Disclosure of related parties and related party transactions

AASB 124 *Related Party Disclosures* requires the disclosure of related party relationships and transactions. To meet the requirements of the standards, management is responsible for implementing internal controls so that:

- all related parties are identified
- all transactions with related parties are identified
- all the disclosures required by the financial reporting framework, including requirements contained in official policies and guidance, are reflected in the financial statements.

3.8.1 Process for identifying and monitoring related parties and related party transactions

The internal controls that are put in place should include the following at a minimum:

- processes to identify and monitor related party relationships
- appropriate approval for transactions to be entered into with a related party
- monitoring controls to identify such transactions and accounting thereof
- appropriate approval of significant or sensitive transactions and arrangements outside the normal course of business.

This could involve employees within an entity declaring conflicts of interests on a regular basis. For this to be effective the entity and its employees must understand the definition of a related party. For local governments, related parties include councillors and senior executives, including their close family members, as well as all their related entities. It is important declarations are obtained from councillors who presided over the financial reporting period. Declarations should be gathered for financial reporting and audit purposes in a timely manner taking into consideration election cycles and potential departures of councillors.

To identify related parties, entities should consider the definition of related party together with relevant policies and guidelines released by public sector regulators such as the Department of Treasury or the Department of Local Government, Sport and Cultural Industries (DLGSC), as appropriate. When related parties are identified, there should be processes in place to monitor transactions with the related party for disclosure purposes.

3.8.2 Auditing related parties

The auditor will need to make sure that all of the related party relationships and transactions that must be disclosed in the financial statements have been included and are consistent with the requirements of the financial reporting framework.

The audit team will need to understand the processes in place to identify these relationships and to identify all transactions with related parties. They will also make enquiries and perform

procedures to check that all the relationships and transactions that need to be disclosed in the financial statements have been included.



A questionnaire is available on line for an entity to complete which will help the audit team better understand an entity's processes for identifying related party relationships and transactions. It can also help the entity identify any weaknesses that may exist in the processes.

3.9 Lead schedules

A lead schedule (also called a lead sheet) is a document that serves as a summary and index of the accounts that make-up financial statement line items and related note disclosures. It is called a lead schedule because traditionally it was the front page in the relevant section of a file, cross referenced to supporting working papers and the documentation filed behind it.

A lead schedule shows the general ledger accounts that are included in each financial statement line item and note disclosure. There would normally be one lead schedule for each financial statement line item or group of related line items. The total on the lead schedule should agree with the final balance in the financial statements.

The lead schedule provides a record of what was included in each financial statement line item. This provides a valuable reference point for an entity's records and can be especially helpful when there are staff changes in a finance team.

Below are some explanations of what to include in each column:

- account code – reference to trial balance
- name – financial statement line item balance name
- source – reference to supporting working paper or documentation
- actual current year – this should agree to the final version of the financial statements
- actual last year – this should agree to the audited version of the prior year financial statements
- budget current year – this should agree to the originally approved budget from the start of the financial year
- variance explanations – reference to explanation for any significant variances.

The lead schedule is also a place where significant movements for the year are explained and recorded for future reference. A good variance explanation would highlight what caused the variance and why. Ideally the impact of each cause is quantified to identify how much of the variance resulted from it. For example, instead of saying salaries increased because we employed more people. It is more useful to say we expanded our contracting business unit by five people and therefore salaries increased by \$250,000.

The variance explanations are also used by the audit team as part of the process of understanding each financial statement line item and identifying potential risks. It is important that the reasons for significant variances are adequately explained so that the financial auditor can understand why there is a variance. The financial audit team may ask further questions and request evidence to corroborate the variance explanations.

Sometimes the reasons for a variance may not be clear at the financial statements line item level, so it is often advisable to break this amount down to the note disclosure level or similar more detailed level in a sub-lead schedule in order to analyse and explain the variance(s).

The lead schedule template, available on our website, includes a worksheet where this can be done.

In some instances, the variance between the actual current year and budget amounts may be the more relevant comparison, while in other instances it may be the variance between the actual current year and the actual prior year. If you have any uncertainty in this area, you should liaise with the audit team.

One way of getting assurance that the lead schedules have been accurately prepared is having a quality assurance review and recording the various steps taken by both the preparer and reviewer. This should be evidenced in the sign-off section on the lead sheet.



A lead schedule template is available from our website to assist in providing a reference to all relevant documents that support each financial statements item or note.

3.9.1 Information required for lead schedules

- Completed lead schedules for each line item in the financial statements.
- Completed sub-lead schedules for all note disclosures relating to each of the line items in the financial statements.
- Descriptions and explanations for the variance identified in the lead schedules between the actual current year amounts when compared to the budgeted and actual prior year amounts.
- Evidence of the review of the lead schedule.

3.10 Property, plant and equipment and infrastructure fair value assessment – State government sector

3.10.1 Background

Depending on the financial reporting regime, an entity can either be required to adopt or may voluntarily choose the revaluation model as its accounting policy that applies to an entire class of property, plant and equipment (PPE) under AASB 116 *Property, Plant and Equipment*. An entity can either be required to adopt or may voluntarily choose the revaluation model as its accounting policy that applies to an entire class of property, plant and equipment (PPE) under AASB 116 *Property, Plant and Equipment*. It will depend on the type of State government entity and which financial reporting regime it operates under (i.e. FMA entities versus non-FMA entities established under statute).

Where the AASB 116 revaluation model applies, it requires a valuation to be undertaken when the carrying amount of items of PPE or infrastructure is materially different from its fair value. Most entities revalue their applicable asset classes on a cyclical basis, which is conditionally allowed under the standard. This means a fair value assessment is still required to be performed in a non-revaluation year to ensure that the carrying amount does not differ materially from fair value in a given financial year, as certain items of PPE or infrastructure may experience significant changes in fair value.

AAS define fair value as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date (see AASB 13 *Fair Value Measurement*).

The State government entity should consider implementing as part of the preparation of financial reports a formal robust process to determine whether indicators exist annually, that would trigger a requirement to perform a formal revaluation of relevant non-financial assets. Where indicators exist a robust fair value assessment should be performed consistent with the requirements of AASB 13. This process is to ensure that the entity's relevant non-financial assets are carried at fair value in compliance with AASB 116 and Treasurer's instructions.

This may entail obtaining relevant input from an independent valuer as to whether or not they consider there are any prevailing market factors which may indicate that the fair value of relevant PPE and infrastructure are likely to have been impacted to any material extent from the prior year. Where a fair value assessment has been performed internally, the entity may consider having this assessment peer reviewed by an independent valuer to obtain assurance over the valuation methodology applied, inputs and the reasonableness of the valuation model applied.

3.10.2 Nature of fair value assessment

A fair value assessment needs to be sufficiently robust so that all requirements of the standards are met. This could also allow for the auditor to rely on some of the work performed (see using the work of an expert). Common examples of the types of fair value assessments undertaken are:

- For land and buildings, Western Australian Land Information Authority (Landgate) usually conducts these valuations annually under their methodology consistent with AASB requirements.
- For other specialised PPE or infrastructure carried at fair value (i.e. current replacement cost basis - infrastructure assets, road networks and similar specialised assets, you may choose to use relevant inflation index (such as CPI) movements or unit rate information to provide an initial indication on whether the fair value has materially changed from the carrying amount). CPI information can be determined by reference to Australian Bureau of Statistics data provided on its website. Unit rate information could come from recent entity-specific contract information or from other external sources.

These percentage movements can be used to work out an estimated fair value movement and whether a revaluation should be performed. However, before completing such an approach, we would recommend that entities discuss the fair value assessment with the audit team.

In a situation where entities have used market based or statistical information to estimate potential fair value movements, we would expect entities to still consider whether these movements are in-line with your expectations. These sources of information could be based on regional data and may not represent local conditions.

Valuations should be factored into the financial statements planning process to ensure they are completed in a timely manner without significantly impacting on an entity's normal operations and processes and audit timeliness, including the preparation of the financial statements.

The auditors are likely to focus on the assumptions used in the fair value assessment and if an external party (expert) has been used may discuss these directly with them.

Whether the fair value assessments are undertaken in-house or externally by suitably qualified and experienced professionals it is essential that the assessments/valuations are specifically completed, and noted as such, for the purposes of financial reporting purposes and in accordance with relevant accounting standards.



The entity is required to complete an information request and return to the auditor.

3.11 Property, plant and equipment and infrastructure fair value assessment – local government sector

3.11.1 Background

Under the Local Government (Financial Management) Regulations 1996 (FM Regulations), certain non-financial assets are required to be shown at fair value in the annual financial report consistent with the AAS. This means that non-financial assets, other than plant and equipment, under AASB 116 *Property, Plant and Equipment* apply the revaluation model that requires a valuation to be undertaken when the carrying amount items of land and buildings, or infrastructure is materially different from its fair value. Most entities revalue their applicable asset classes on a cyclical basis, which is conditionally allowed under the standard. This means a fair value assessment is still required to be performed in a non-revaluation year to ensure that the carrying amount does not differ materially from fair value in a given financial year, as certain items of PPE or infrastructure may experience significant changes in fair value.

AAS define fair value as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date (see AASB 13 *Fair Value Measurement*).

The local government entity should consider implementing as part of the preparation of financial reports a formal robust process to determine whether indicators exist annually, that would trigger a requirement to perform a formal revaluation of relevant non-financial assets. Where indicators exist a robust fair value assessment should be performed consistent with the requirements of AASB 13. This process is to ensure that the local government's relevant non-financial assets are carried at fair value in compliance with AASB 116 and the FM Regulations.

This may entail obtaining relevant input from an independent valuer as to whether or not they consider there are any prevailing market factors which may indicate that the fair value of relevant PPE and infrastructure are likely to have been impacted to any material extent from the prior year. Where a fair value assessment has been performed internally, the local government entity may consider having this assessment peer reviewed by an independent valuer to obtain assurance over the valuation methodology applied, inputs and the reasonableness of the valuation model applied.

3.11.2 Nature of fair value assessment

A fair value assessment needs to be sufficiently robust so that all requirements of the standard are met. This could also allow for the auditor to rely on some of the work performed (see using the work of an expert). Common examples of the types of fair value assessments undertaken are:

- For non-specialised PPE required to be carried at fair value (i.e. land and buildings), a review of similar property sale figures for the relevant period or other market-based information. Valuers can provide estimates of property price increases.
- For specialised PPE and infrastructure required to be carried at fair value (i.e. current replacement cost basis), such as infrastructure assets, roads, drainage, pathways, parks and reserves, and other infrastructure, you may choose to use relevant inflation

index such as CPI movements or unit rate information to provide an initial indication on whether the fair value has materially changed from the carrying amount. CPI information can be determined by reference to Australian Bureau of Statistics data provided on its website. Unit rate information could come from recent entity-specific contract information or from other external sources.

These percentage movements can be used to work out an estimated fair value movement and whether a revaluation should be performed. However, before completing such an approach, we would recommend that entities discuss the fair value assessment with the audit team.

In a situation where entities have used market-based or statistical information to estimate potential fair value movements, we would expect entities to still consider whether these movements are in-line with your expectations. These sources of information could be based on regional data and may not represent local conditions.

Valuations should be factored into the financial report planning process to ensure they are completed in a timely manner without significantly impacting on an entity's normal operations and processes and audit timelines, including the preparation of the financial report.

The auditors are likely to focus on the assumptions used in the fair value assessment and if an external party has been used may discuss these directly with them.

Whether the fair value assessments are undertaken in-house or externally by suitably qualified and experienced professionals it is essential that the assessments/valuations are specifically completed, and noted as such, for the purposes of financial reporting purposes and in accordance with relevant accounting standards.

You should only engage accredited valuers who are qualified to perform valuations of the relevant assets for financial reporting purposes. The resulting valuation reports should clearly state that the valuation is in accordance with the AAS and FM Regulations.

In the intervening period between scheduled formal revaluations, each year entities should assess whether the relevant asset classes' carrying amounts differ materially from fair value at the reporting date, as required by the AAS and FM Regulations, and determine whether an interim revaluation is necessary.

Interim desktop revaluations can be considered only if the source information (i.e. indices) are reliable and accurate, and if a desktop valuation considers all material factors. If entities do not have the capability or required information to perform a desktop review, they need to consider engaging a management expert or external valuer early in the process.



The entity is required to complete an information request and return to the auditor.

3.12 Impairment of assets

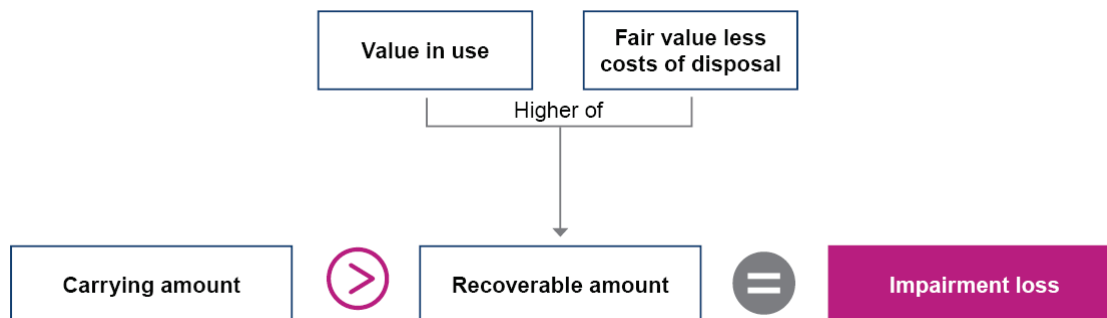
This section primarily considers the requirements of AASB 136 *Impairment of Assets*. The standard applies to public sector entities accounting for the impairment of assets such as:

- property, plant and equipment
- infrastructure
- intangible assets.

3.12.1 Overview

The standard requires an entity to recognise an impairment loss when its assets are carried at more than their recoverable amount. The standard prescribes procedures that an entity has to apply to ensure assets are carried at no more than their recoverable amount.

At each reporting date, an entity is required to assess whether there is an indication that an asset may be impaired.



Source: OAG

Figure 1: Determining an impairment loss

3.12.2 Key definitions

Impairment: occurs where an asset is carried at more than its recoverable amount.

Impairment loss: the amount by which the carrying amount of an asset that is not part of a cash-generating unit exceeds its recoverable amount.

Carrying amount: the amount at which an asset is recognised in the statement of financial position, after deducting any accumulated depreciation and accumulated impairment losses thereon.

Recoverable amount: the amount that is the higher of an asset's fair value less costs of disposal and the assets value in use.

Fair value less costs of disposal: the price that would be received to sell an asset in an orderly transaction between market participants at measurement date, less costs of disposal.

Value in use: the present value of the future cash flows expected to be derived from an asset.

Costs of disposal: incremental costs directly attributable to the disposal of an asset, excluding finance costs and income tax expense.

3.12.3 So how do you apply the requirements of AASB 136 to your entity?

Under AASB 136 (paragraph Aus5.1), many assets of not-for-profit entities are not held primarily for their ability to generate net cash inflows – rather they are specialised assets held for continuing use of their service capacity / service delivery.

Specialised assets will have very limited or no alternative use and/or be substantially customised to facilitate the delivery of particular public services. Specialised assets would ordinarily include various types of infrastructure, specialised buildings (e.g. prisons, hospitals, schools), and major plant and equipment that is substantially customised.

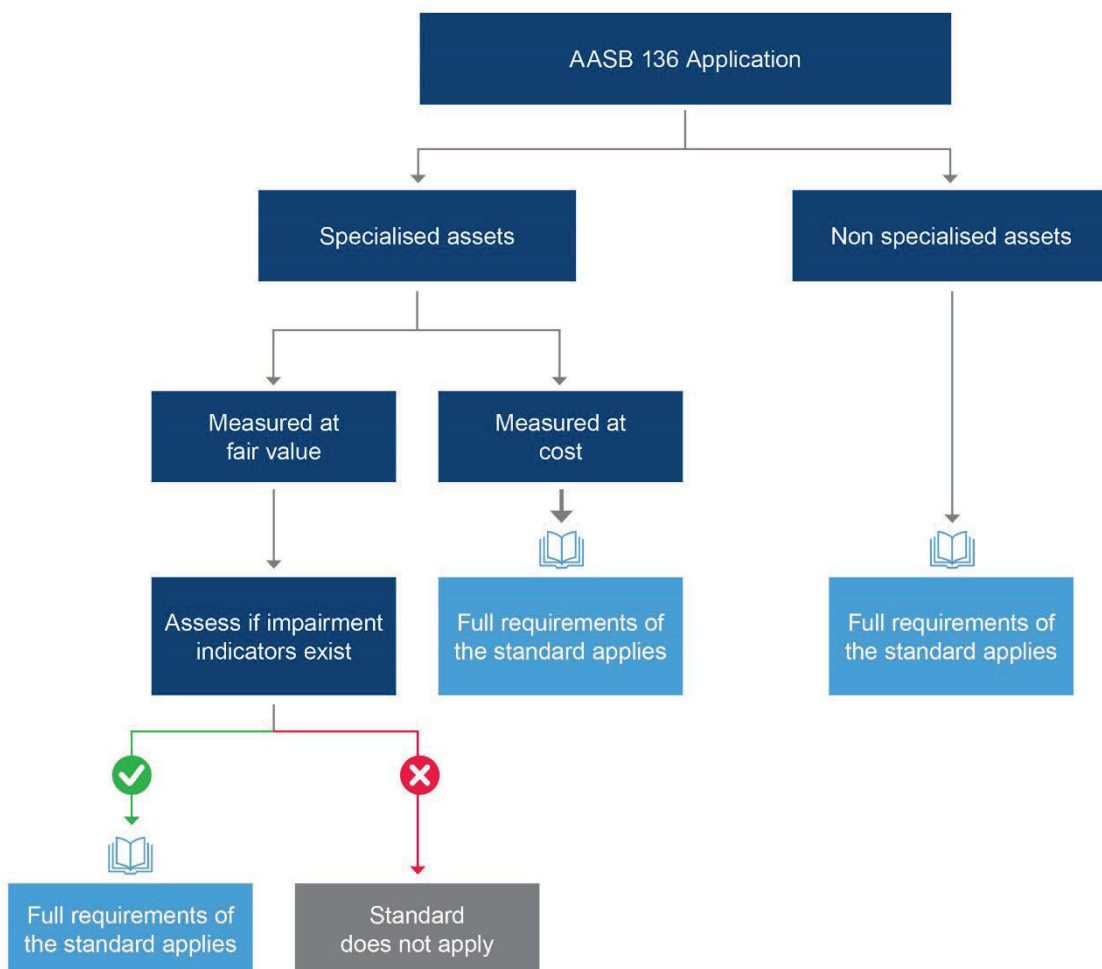
AASB 136 (paragraph Aus5.1) specifies that because such specialised assets of not-for-profit entities are rarely sold, their cost of disposal is typically negligible. Consequently, the recoverable amount of such specialised assets is expected to be materially the same as fair value, determined under AASB 13 *Fair Value Measurement*.

However, not-for-profit entities must continue to assess every year at reporting date whether there are any indicators that the service capacity of its assets have changed since the last revaluation was completed. Where indicators exist that the asset has experienced a material reduction in service capacity or remaining useful life since the effective date of the last valuation, the fair value of the asset should be reviewed and, if required, adjusted downwards.

For specialised assets measured at cost under AASB 116 and AASB 138 *Intangible Assets* and all other non-specialised assets (including work-in-progress) and assets held for generating cash flows (in the rare circumstances cash-generating assets are held by not-for-profit entities) under AASB 116 and AASB 138, the requirements of AASB 136 applies.

For non-specialised assets measured at fair value (or an amount that approximates fair value), impairment would only arise in rare circumstances such as where the costs of disposal are material. Similar to specialised assets measured at fair value, any impairment of these assets is also effectively captured through the revaluation process. Note that impairment is one factor that the desktop valuation does not cover. Therefore, if a desktop revaluation is performed, you would be expected to conduct annual assessments of impairment indicators as normally required and recognise impairment losses if necessary (as a separate exercise from the desktop revaluation).

In summary, AASB 136 applies to not-for-profit entities, as follows:



Source: OAG

Figure 2: AASB 136 Application flowchart

Consistent with the above, at each reporting date, an entity is required to assess whether there is an indication that an asset may be impaired. A list of external and internal impairment indicators are described in AASB 136. If there is an indication that the entity's asset(s) may be impaired, then the asset(s) recoverable amount must be estimated, and an impairment loss recognised where required.

Irrespective of whether there is any indication of impairment, an entity must test an intangible asset with an indefinite useful life or an intangible asset not yet available for use for impairment annually by comparing its carrying amount with its recoverable amount.

Examples of impairment indicators are:

- External sources of information:
 - cessation, or near cessation, of the demand or need for services provided by the asset
 - significant adverse changes expected in terms of technological advances, market, economic, legal, or government policy environment.
- Internal sources of information:
 - obsolescence and/or physical damage
 - significant changes, expected and occurred, in the entity resulting in the assets becoming idle or impacting on its remaining useful life
 - discontinuing or restructuring of the operations to which an asset belongs
 - internal evidence that the performance of an asset will be worse than expected.

These examples are not intended to be exhaustive. An entity may identify other indications that an asset may be impaired and these would also require the entity to determine the asset's recoverable amount.

3.12.4 Measuring recoverable amount

It is not always necessary to determine both an asset's fair value less costs of disposal and its value in use. If either of these amounts exceeds the asset's carrying amount, the asset is not impaired, and it is not necessary to estimate the other amount.

3.12.5 Fair value less costs of disposal

An asset's fair value less costs of disposal is the price at which an orderly transaction to sell the asset would take place between market participants at measurement date under current market conditions, adjusted for incremental costs that would be directly attributable to the disposal of the asset.

Fair value is to be measured under AASB 13.

Costs of disposal include costs of removing the asset and direct incremental costs to dispose of the asset.

3.12.6 Value in use

The present value of the future cash flows expected to be derived from a non-cash generating asset (including its ultimate disposal) would normally be approximately nil.

3.12.7 Recognition of an impairment loss

If, and only if, the recoverable amount of an asset is less than its carrying amount, the carrying amount of the asset shall be reduced to its recoverable amount. That reduction is an

impairment loss. An impairment loss shall be recognised immediately in surplus or deficit unless the asset is carried at a revalued amount in accordance with another standard (e.g. the revaluation model in AASB 116). Any impairment loss of a revalued asset shall be treated as a revaluation decrease in accordance with the other standard.

For not-for-profit entities, an impairment loss on a revalued asset is recognised in other comprehensive income to the extent that the impairment loss does not exceed the amount in the revaluation surplus for the class of asset. Such an impairment loss on a revalued asset reduces the revaluation surplus for the class of asset.

3.12.8 Reversal of impairment

An entity shall assess at each reporting date whether there is any indication that an impairment loss recognised in prior periods for an asset may no longer exist or may have decreased. If any such indication exists, the entity shall estimate the recoverable amount of that asset.

The same approach is followed as for the identification of impaired assets i.e. assess at the end of each reporting period whether there is an indication that an impairment may no longer exist or may have decreased using impairment indicators. If there is evidence of a decrease in impairment, calculate the recoverable amount.

An impairment loss recognised in prior periods for an asset shall be reversed if, and only if, there has been a change in the estimates used to determine the asset's recoverable amount since the last impairment loss was recognised. If this is the case, the carrying amount of the asset shall be increased to its recoverable amount (subject to the ceiling, as described below). That increase is a reversal of an impairment loss.

The increased carrying amount of an asset attributable to a reversal of an impairment loss shall not exceed the carrying amount that would have been determined (net of amortisation or depreciation) had no impairment loss been recognised for the asset in prior years (the ceiling).

A reversal of an impairment loss for an asset shall be recognised immediately in surplus or deficit unless the asset is carried at a revalued amount in accordance with another standard (e.g. revaluation model in AASB 116). Any reversal of an impairment loss shall be treated as a revaluation increase in accordance with that other standard.

For not-for-profit entities, a reversal of an impairment loss on a revalued asset is recognised in other comprehensive income and increases the revaluation surplus for the class of asset. However, to the extent that an impairment loss on the same class of asset was previously recognised in surplus or deficit, a reversal of the impairment loss is also recognised in surplus or deficit.

3.12.9 What are the disclosure requirements of AASB 136?

Disclosure by class of assets:

- the amounts of impairment losses recognised in surplus or deficit
- the amounts of impairment losses reversed in surplus or deficit
- the line item(s) of the statement of comprehensive income in which those impairment losses and reversals are included.

Other disclosures:

An entity shall disclose the following for an individual asset for which a material impairment loss is recognised or reversed during the reporting period:

- events and circumstances resulting in the impairment loss or reversal
- amount of the impairment loss or reversal
- the nature of the asset
- whether the recoverable amount is its fair value less costs of disposal or value in use
- if the recoverable amount is fair value less costs of disposal, the following information:
 - fair value measurements categorised within level 2 and level 3 of the fair value hierarchy (see AASB 13)
 - a description of the valuation techniques used to measure fair value less costs of disposal
 - for any change in valuation technique, the reasons for making it
- if no information is disclosed for the above other disclosures (due to individual assets impairment losses and/or reversals not being material), the entity is to disclose the following information for the aggregate impairment losses and aggregate reversals during the reporting period:
 - the main classes of assets affected
 - the main events and circumstances that led to the recognition of these impairment losses and reversals.

3.12.9 Management's responsibility for recognition of impairment losses and reversals

Management is responsible for the identification, recognition and disclosure of impairment losses and reversals. This responsibility requires management to implement adequate accounting and internal control systems to ensure that impairment is appropriately identified and disclosed, where appropriate, in the financial reports.

Management would normally engage an expert to determine the fair value less costs of disposal and the value in use. It is management's responsibility to ensure that the information provided to the expert is complete and accurate. Where management has performed the calculation of the value in use there should be adequate evidence to support the assumptions made by management/expert.

3.12.10 Systems for identifying and monitoring impairment assessment

We expect entities to establish systems and internal controls to:

- perform cyclical counts/physical inspections of assets and maintain an up-to-date fixed asset register of all assets
- identify, account for, monitor and disclose impairment in accordance with the applicable financial reporting framework (i.e. AASB 136)
- review and approve the expert reports and calculations prepared for the value in use and the expert reports for the fair value less costs of disposal assessments
- formally authorise and approve the assessments that have been prepared.



The entity is required to complete an information request and return to the auditor.

3.13 Using the work of an expert

3.12.1 Background

An entity may engage the services of an external party expert or an internal expert, to provide assistance to determine financial and/or non-financial information for use in the financial statements or KPIs. For example, an independent external valuer may be engaged to revalue land and buildings or infrastructure assets, and for KPIs a market research company may carry out a survey. Internal engineers may be requested to value infrastructure.

3.13.2 Management's responsibilities

When an entity engages an expert, it is important that the management of the entity continues to take ownership of the process as the information determined by the expert will be included in the financial statements or KPIs. An entity must also ensure that the expert understands the requirements and keeps adequate records of their work. Financial auditors may have important questions on the process and may need further explanations.

An entity may also need to provide an expert with certain data or reports from its financial management information systems and performance information systems. It is important that management ensures that complete and accurate data and information is provided to the expert when this is going to be used by the expert in performing their work. Management should be able to explain to the financial auditors what procedures they performed over the information and data that was provided to the expert. The financial auditor may also perform certain audit procedures on this information and data.

Management should have adequate processes and controls around expert reports, to ensure they have a reasonable understanding of the methodology, inputs and assumptions, and final outcomes, and challenge these where required. This also includes management engaging experts that are competent and independent.

When engaging an expert, it is generally advisable to liaise with your financial auditor to ensure the intended scope will satisfy relevant requirements for financial reporting purposes, prior to engaging the expert.

3.13.3 Financial auditors' area of focus

Where an entity has engaged an expert, the financial auditor may use the expert's work as audit evidence. To complete this piece of work, as outlined in auditing standards, the auditor must assess and test (where appropriate) the following for the work performed by the expert:

- Is the expert professionally competent?
- Is the expert objective?
- Obtain an understanding of what work the expert has done.
- Is the scope of work performed by the expert adequate for that piece of work, and in line with applicable AAS and/or other requirements?
- Assess the appropriateness of the expert's work, including consideration of:

- Has the correct source data been used and is it complete and accurate?
- Is the methodology appropriate?
- Are the assumptions used appropriate?
- Relevance and reasonableness of the findings or conclusions.

The financial auditor will complete this piece of work by requesting some information from the expert. The financial auditor's requests would usually ask the expert to confirm/provide:

- their qualifications and experience
- their objectivity
- their compliance with relevant professional standards
- whether they believe their work is in compliance with AAS and/or other relevant requirements
- whether they believe their work is appropriate for inclusion in the financial statements or KPIs
- they are aware that the financial auditor will be using their work in forming the auditor's opinion
- to provide a copy of the expert's report
- to provide information regarding assumptions, methods and criteria (if not in the report).

In some instances, where an auditor requires further clarification from the expert, the auditor may request to meet with the expert. When an entity engages an expert for financial and/or non-financial information, it is important that the entity explains to the expert that the auditor may contact them.

It is also recommended that the entity advise the auditor early if it plans to engage an expert, this will allow the financial auditor to discuss with the entity what specific areas the financial auditor will focus on in relation to the work of the expert and ensure the scope is appropriate.



The entity is required to complete an information request and return to the auditor.

3.14 Changes in accounting policy and estimates, and prior period errors

3.14.1 Background

Accounting policies are the specific principles, bases, conventions, rules and practices applied by an entity in preparing and presenting financial statements (AASB 108 *Accounting Policies, Changes in Accounting Estimates and Errors*). Accounting policies when applied consistently and in accordance with accounting standards, increase the relevance and reliability of the financial statements and comparability of the financial statements over time and with other entities.

Accounting policies may change from time to time as a result of changes in requirements under AAS or when an entity voluntarily decides to improve or enhance the relevance and reliability of the results and information contained in the financial statements. Where no

specific AAS applies to a transaction, entities may also consider applying accounting policies to those transactions based on guidance from other jurisdictions. Any subsequent changes in such accounting policies resulting from amendments to the underlying guidance are considered to be voluntary changes in accounting policy.

Changes in accounting policies shall be applied as follows:

- on initial application of an AAS – in accordance with the specific transitional provisions (if any)
- on initial application of an AAS – if no specific transitional provisions apply to the change, the changes are applied retrospectively (except to the extent that it is impracticable)
- changes are made voluntarily – the change is applied retrospectively (except to the extent that it is impracticable).

AASB 108 requires disclosures when a change in accounting policy occurs and depending on the nature of the change, disclosure requirements vary. Entities should refer to AASB 108 for the relevant requirements.

Accounting estimates are monetary amounts for items in financial statements that cannot be measured with precision but can only be estimated based on the latest available, reliable information (AASB 108). Entities may need to develop a reasonable estimate for certain financial statement line items where there is no directly observable data or inputs available. Such items are subject to uncertainty and involve the use of judgements and assumptions based on the best information available. Common examples of accounting estimates include, fair values of an asset or liability, depreciation expense for property, plant and equipment, and infrastructure assets, employee benefits provision and provision for rehabilitation costs.

Changes in accounting estimates generally occur as a result of new information, developments or more experience which require an update to inputs and/or change in measurement technique. For example, an underlying input of the fair value measurement of an infrastructure asset such as CPI or supplier contract pricing may materially change from the previous financial year, triggering a refresh of the fair value assessment of infrastructure assets in the current financial year. A change in accounting estimates apply prospectively. This is distinguished from a change in the measurement basis applied, which is a change in accounting policy and not a change in accounting estimate.

AASB 108 requires disclosures of the nature and amount of a change in an accounting estimate that has an effect in the current period or is expected to have an effect in future periods to the extent it is practicable to estimate the effect on future periods.

According to AASB 108, prior period errors are omissions from, and misstatements in, the entity's financial statements for one or more prior periods arising from a failure to use, or misuse of, reliable information that:

- was available when financial statements for those periods were authorised for issue
- could reasonably be expected to have been obtained and considered in the preparation and presentation of those financial statements.

Such errors include the effects of mathematical mistakes, mistakes in applying accounting policies, oversights or misinterpretations of facts, and fraud (AASB 108).

Errors can relate to recognition, measurement, presentation or disclosure of elements of financial statements. If financial statements contain material errors or immaterial errors made intentionally to achieve a particular presentation of an entity's financial statements, they are regarded as not complying with AAS. Generally, current period errors discovered in that

period are corrected before the financial statements are authorised for issue. However, material errors that are discovered in subsequent periods require correction in the comparative information presented in the financial statements for that subsequent period.

Prior period errors are corrected retrospectively by restating the comparative amounts for the prior period in which the error occurred or if the error occurred before the earliest period, restating the opening balances of assets, liabilities and expenses for the earliest prior period presented (except to the extent that it is impracticable).

AASB 108 requires specific disclosures for all material prior period errors in addition to corrections to reported balances and disclosures. Entities should refer to AASB 108 for the details of the disclosure requirements. Financial statements of subsequent periods need not repeat these disclosures. In recent times, we have observed prior period errors arising in respect of property, plant and equipment, and infrastructure asset recognitions and revaluations.

3.14.2 Financial auditors' expectations and requirements

Where an entity has identified an accounting policy change, change in accounting estimate or prior period error, the auditor requires management to provide position papers and supporting documentation for the change and the financial impact.

It is management's responsibility to present to the auditor the effects of a change in accounting policy and estimates, and any prior period errors identified in the current year financial statements and have it appropriately reviewed and signed off before presenting it for audit. Accounting position papers are an important tool that entities can use to document key decisions and to keep stakeholders, such as senior management, auditors and audit and risk committees apprised of updates to accounting policies and processes, and how they affect the financial statements. Accounting position papers should document all the matters considered when making the decision. Further information on accounting position papers can be found in our *Western Australian Public Sector Financial Statements – Better Practice Guide*.

Position papers should be reviewed and signed off by appropriate finance team staff before submitting it to the auditors.



If applicable, a position paper template is available on our website that can be tailored to your circumstances.

3.15 General computer controls

General computer controls (GCC) audit is an integral part of our financial audits. The objective of GCC audits is to determine if entities' computer controls effectively support the preparation of financial statements, delivery of key services and the confidentiality, integrity and availability of information systems. Well operating controls help entities protect their information systems and IT environments from data breaches and cyber security threats.

These audits provide assurance over the following general computer controls:



Figure 3: General computer control categories

Source: OAG

Auditor General's 2022-23 reports

Number	Title	Date tabled
25	Traffic Management System	14 June 2023
24	Security Basics for Protecting Critical Infrastructure from Cyber Threats – Better Practice Guide	14 June 2023
23	Contractor Procurement – Data Led Learnings	14 June 2023
22	Effectiveness of Public School Reviews	24 May 2023
21	Financial Audit Results – State Government 2021-22 – Part 2: COVID-19 Impacts	3 May 2023
20	Regulation of Air-handling and Water Systems	21 April 2023
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation of Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
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

This page is intentionally left blank

This page is intentionally left blank

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

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

www.audit.wa.gov.au



@OAG_WA



Office of the Auditor General
for Western Australia

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Biannual Compliance Task Report

RISK THEME PROFILE:

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

RISK ASSESSMENT CONTEXT: Strategic

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

Internal Audit Strategic Plan

2023/24 – 2025/26



Document Control					
Document ID: Internal Audit Strategic Plan					
Rev No	Date	Revision Details	Author	Approver	Adopted
1.0	01/07/2019	Original plan created and adopted	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	OCM 14-08-2019 Res 251-19
2.0	23/06/2020	Annual update of plan	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	OCM 30-09-2020 Res 280-20
3.0	03/08/2021	Annual update of plan	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	OCM 29-09-2021 Res 304-21
4.0	14/09/2022	Annual update of plan	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	OCM 28-09-2022 Res 250-22
5.0	13/09/2023	Annual update of plan	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	Scheduled for OCM 27-09-2023 Res Pending

Contents

<i>Introduction.....</i>	<i>1</i>
<i>Internal Audit Activities Overview.....</i>	<i>1</i>
<i>Methodology.....</i>	<i>3</i>
<i>Internal Audit Coverage Prioritisation</i>	<i>4</i>
<i>Objective</i>	<i>4</i>
<i>Responsibilities.....</i>	<i>5</i>
<i>Auditor General Reports</i>	<i>5</i>
<i>Internal Audit Annual Work Plan</i>	<i>6</i>
<i>Annual Audit Review 2023-2024.....</i>	<i>7</i>
<i>Template – Internal Audit Assessment and Response Summary</i>	<i>8</i>

Introduction

The primary purpose of the Shire of Dardanup's Internal Audit Plan is to align its focus and activities on the Council's key internal risks. The Internal Audit functional planning framework consists of two key elements:

- an Internal Audit Strategic Plan with a three-year outlook that relates the role of internal audit to the requirements of the Council by outlining the broad direction of internal audit over the medium term, in the context of all the Council's assurance activities; and
- an Internal Audit Annual Work Plan which includes an Internal Audit Annual Work schedule.

Together, these plans serve the purpose of setting out, in strategic and operational terms, the broad roles and responsibilities of Internal Audit and identify key issues relating to internal audit capability, such as the required professional skills.

This Annual Work Plan covers a financial year in line with the Council's annual budgeting and planning cycle and specifies the proposed internal audit coverage within the financial year.

It is reviewed annually by the Deputy CEO in the first quarter of each financial year and presented to the Audit and Risk Committee for endorsement.

Internal Audit Activities Overview

It is important that internal audit has a predominant focus on the conduct of assurance and advisory activities. Nevertheless, audit support activities are also important activities generally undertaken by Internal Audit.

The relative proportion of resources devoted to audit support activities, compared with audit assurance and advisory activities, is an important matter for consideration by the Audit and Risk Committee when considering Internal Audit plans and budgets.

It is important to note that the smaller the size of the in-house Internal Audit team, the greater the proportion of the audit support activities will be.

Internal Audit conducts the following audit support activities which are generally non-discretionary:

- Internal Audit strategic and operational planning.
- Internal Audit functional and administrative reporting.
- Monitoring the implementation of audit recommendations made by Internal Audit and the External Auditor.
- Liaison with the External Auditor.
- Internal Audit Quality Assurance and Improvement Program.

- Performing any appropriate special tasks or projects requested by the Deputy CEO, CEO or the Audit and Risk Committee.
- Disseminating better practice and lessons learnt arising from the internal audit activities across local government.

The Internal Audit **assurance activities** include engagements with the following orientation:

- **Financial**
 - Auditing the financial statements of externally funded grants including research, capital and other special purpose grants/programs; and
 - Auditing the special purpose financial statements of discrete business operations such as Eaton Recreation Centre.

In performing financial statement audits, Internal Audit typically provides an audit opinion and a reasonable level of assurance to parties outside the Council, depending on the purpose for which the financial statements are prepared.

- **Compliance**
 - Compliance has traditionally been a focus area for Internal Audit activities. The objective of a compliance engagement is to enable Internal Audit to express an opinion on whether the Council or an organisational area has complied in all material aspects, with requirements as measured by the suitable criteria which include:
 - Federal and State legislation and regulatory requirements.
 - Federal and State Government policies and administrative reporting guidelines.
 - Council policies, procedures, and Code of Conduct.
 - contracts to which the Council is a part.
 - strategic plans, or operational programs.
 - ethics related objectives and programs; and
 - other standards and good practice control models.
- **Performance (improvement)**
 - Performance (improvement) engagement is designed to assess the economy, efficiency and effectiveness of the Council's business systems and processes.

A compliance or performance (improvement) engagement is conducted either as an audit, which provides reasonable assurance, or as a review, which provides limited assurance.

For all assurance activities, Internal Audit observes, where applicable, the professional practice guidelines or statements issued by relevant professional bodies, including (but not limited to):

- CPA Australia; and

- Chartered Accountants Australia and New Zealand.

The Internal Audit **advisory activities** are to provide objective and relevant review services or ad hoc advice to management without assuming management responsibility.

The Deputy CEO considers accepting proposed review engagements based on the engagement's potential to improve the management of risks, add value, and improve the Council's operations.

Internal Audit applies the principle that issue prevention activities are more beneficial and could be more cost-effective than issue detection activities. Accordingly, Internal Audit acts proactively in providing ad hoc advice to utilise its control and risk evaluation skills in preventing control weaknesses and breakdowns by providing ad hoc advice to the Council's management on a range of matters, including:

- development of new programs and processes.
- risk management; and
- fraud control.

The percentages of Internal Audit effort to conduct audit support, assurance and advisory activities will fluctuate over the years depending on the Council's assurance needs and the Internal Audit's operational needs and priorities such as system, process, and staff professional development requirements. This is monitored by the Audit and Risk Committee.

Methodology

Internal Audit adopts a **risk-based methodology**. The planning at both the functional and engagement levels is based on the risk assessment performed to ensure that it is appropriate to the size, functions and risk profile of the Council.

In order to provide optimal audit coverage to the Council and minimise duplication of assurance effort, due consideration is given to the following aspects:

- key Council business risks.
- any key risks or control concerns identified by management.
- assurance gaps and emerging needs; and
- scope of work of other assurance providers, internal and external.

Internal Audit maintains an open relationship with the external auditor and other assurance providers.

Internal Audit Coverage Prioritisation

During each financial year, the Internal Audit coverage will have a different focus depending on the Council's current risk profile and assurance needs. The Internal Audit coverage is categorised into the following broad groups. The order in which these are listed is in line with the current priority given to each group based on the risk assessment.

1. **Annual audits** to review key areas of financial, operational, and human resources across the whole Council. This group of engagements are treated as first priority audits to meet the external reporting and compliance obligation of the Council, which can include:
 - a. Grant Audits.
 - b. Direct assistance to external audit by performing audit or review procedures under the direction of the external auditor; such activities customarily include the following engagements:
 - i. Salaries Audit.
 - ii. Expenditure Audit.
 - iii. Revenue Audit; and
 - iv. Follow up on audit recommendations made by the external auditor.
2. Audits of **high-risk areas/systems** where the controls are considered to be effective, however, independent assurance is required to ensure that the controls are in fact operating as intended.
3. Audits that review particular topics **across the whole Council** – such as supplier selection and WHS management framework. This group of engagements are aimed at addressing systemic risks.
4. Audits that review **particular processes/activities** owned by a particular Directorate or Divisions such as gym membership; and
5. Consultancy/ad hoc advice on new systems, processes, and initiatives.

A small contingent time budget may be set aside to accommodate ad hoc or special requests, particularly those from the CEO and the Audit and Risk Committee.

Objective

Engagement objectives are broad statements developed by Internal Audit that define intended engagement accomplishments. This is largely informed by the identified risks and assurance needs of the Council upon commencing of an engagement. Internal Audit provides opportunities for auditees to have input in formulating audit objective(s). For high-risk audits, Internal Audit also seeks the CEO's endorsement of the audit objective(s).

Engagement scope is driven by:

- the determined objectives; the broader the objectives, the wider the audit scope; and
- the level of assurance required; an "audit" provides a reasonable level of assurance and requires wider scope than that for a "review" which provides limited level of assurance.

Responsibilities

The Internal Audit program is to be undertaken by the Shire of Dardanup Senior Corporate Governance Officer, with oversight by the Deputy CEO and assistance of other Council staff when required or available.

Council staff involved with the Internal Audit program will have access to all areas of the Shire of Dardanup operations, including correspondence, files, accounts, records, and documents as is necessary to perform the duties of the role, except those items that are noted as confidential and/or personal. Access to material noted as confidential and/or personal will only be provided upon request by the CEO.

Council staff involved with the Internal Audit program will conduct their reviews based on the methodology and internal audit coverage prioritization contained within the Internal Audit Plan, and report on the outcome of this review. Where it is reported that problems exist, corrective action will be recommended and followed through for action, ensuring that resources are directed towards areas of highest risk.

The Shire of Dardanup Internal Audit Plan will be reviewed and assessed on an annual basis. The Internal Audit Plan may be adjusted as a result of receiving requests to undertake special advisory services to conduct reviews that do not form part of the structured plan.

At the conclusion of each internal audit a report on the outcome will be forwarded to the Deputy CEO. This report will outline what auditing actions were actually taken, provide recommendations for corrective action as required, monitoring, and reporting on the corrective actions undertaken.

Auditor General Reports

The *Local Government Amendment (Auditing) Act 2017* was proclaimed on 28 October 2017. The purpose of the Act was to make legislative changes to the *Local Government Act 1995* to provide for the auditing of local governments by the Auditor General.

The Act also provides for a new category of audits known as 'performance audit reports' which examine the economy, efficiency, and effectiveness of any aspect of a local government's operations. The findings of these audits are likely representative of issues in other local government entities that were not part of the sample. In addition, the Auditor General releases 'guides' to help support good governance within a local government's operations.

The Auditor General encourages all entities, not just those audited, to periodically assess themselves against the risks and controls noted in each of the performance audit reports and guides when published. Testing performance against the Auditor General findings and reporting the outcomes to the Audit and Risk Committee can be further viewed as a vital component of the internal control function under Regulation 17.

Internal Audit Annual Work Plan

INTERNAL AUDIT ANNUAL WORK SCHEDULE 2023-2024					
PROJECT	TYPE	RISK RATING	BUDGET DAYS	DATE	RESOURCES
Process Mapping	Process Review	Moderate	One year	July 2023 to June 2024	ERP Project Manager Senior Corporate Governance Officer
IT Hardware and Software Review	Assurance – Financial; Compliance	Moderate	10 days	November 2023	Senior Corporate Governance Officer

Annual Audit Review 2023-2024

Process Review

Process Mapping

- Work with the external consultant to map the current state of business processes to support the Enterprise Resource Planning (ERP) implementation timeline.
- Identify weaknesses or deficiencies that need to be rectified prior to transition to new ERP.

Assurance – Financial; Compliance

IT Hardware and Software Review

- Review IT Hardware and Software Inventory list to ensure all items are managed in accordance with Administration Policy AP024 Information Technology Management, in particular:
 - Custodianship and management of items.
 - New IT hardware and software requests have met the security assessment/acceptance process and approval subsequently granted by the Manager Information Services or DCEO.
- Extend the review for items which may have been procured without due consideration for AP024, by:
 - Reviewing the Portable and Attractive Items Register (PAIR – items < \$5k).
 - Reviewing the Asset Register (items > \$5K).
 - Perform a sample testing against departmental IT Software, Hardware and Support expenditure accounts.

Template – Internal Audit Assessment and Response Summary

SHIRE OF DARDANUP – INTERNAL AUDIT ASSESSMENT AND RESPONSE SUMMARY		
Prepared by Date Audit Focus Area		
ASSESSMENT	OBJECTIVES MET Yes/No/NA	COMMENTS
C1 Internal Controls C1.1 Ownership C1.2 Comprehensive Written Procedures C1.3 Confirm Staff Aware of Procedures C1.4 Confirm Staff Follow Procedures		
C2 Transaction Verification		
C3 Authorising Process		
C4 Processing		
C5 Compliance		
C6 Payments		
Reviewed by Date Signed		

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: 2023-2024 Internal Audit Program

RISK THEME PROFILE:

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

9 - External Theft and Fraud (including Cyber Crime)

8 - Errors, Omissions and Delays

12 - Misconduct

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Not considering internal control within the organisation would result in non-compliance with Regulation 17	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.



Our Ref: 8658

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

Mr Andre Schonfeldt
Chief Executive Officer
Shire of Dardanup
P O Box 7016
EATON WA 6232

Mail to: Perth BC
PO Box 8489
PERTH WA 6849

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

Dear Mr Schonfeldt

**ANNUAL FINANCIAL REPORT
INTERIM AUDIT RESULTS FOR THE YEAR ENDED 30 JUNE 2023**

We have completed the interim audit for the year ended 30 June 2023. We performed this phase of the audit in accordance with our audit plan. The focus of our interim audit was to evaluate your overall control environment, but not for the purpose of expressing an opinion on the effectiveness of internal control, and to obtain an understanding of the key business processes, risks and internal controls relevant to our audit of the annual financial report.

The result of the interim audit was satisfactory. An audit is not designed to identify all internal control deficiencies that may require management attention. It is possible that irregularities and deficiencies may have occurred and not been identified as a result of our audit.

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

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

Feel free to contact me on 6557 7551 if you would like to discuss these matters further.

Yours faithfully

Suraj Karki
Acting Director
Financial Audit
7 June 2023

Attach

(Appendix AAR: 8.4B)

RISK ASSESSMENT TOOL									
OVERALL RISK EVENT:		Annual Financial Report – Interim Audit Results for the Year Ending 30 June 2023							
RISK THEME PROFILE:									
3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)		12 - Misconduct							
8 - Errors, Omissions and Delays		Choose an item.							
RISK ASSESSMENT CONTEXT:		Operational							
CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL			RESIDUAL RISK RATING
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD		
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Not presenting the Interim Audit Results for the year ending 30 June 2023 to the Audit and Risk Committee (and subsequently Council).	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council’s reputation could be seen in a negative light for not being open and transparent with disclosing findings from the Auditor General.	Minor (2)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.	Not required.
PROPERTY	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.	Not required.

