



Shire of Dardanup

APPENDICES

AUDIT & RISK COMMITTEE MEETING

To Be Held

Wednesday, 2 September 2020
Commencing at 3.00pm

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			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 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.	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.	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.

Western Australian Auditor General's Report



Controls Over Purchasing Cards

**Office of the Auditor General
Western Australia**

Audit team:

Carly Meagher
Joanne Clarke
Carol Brownfield
Fatima Padia
Charmain Lin
Michelle Lai
Paula Du Plessis
Jojo Liew

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

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

© 2020 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Controls Over Purchasing Cards



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

CONTROLS OVER PURCHASING CARDS

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

This focus area audit assessed if sampled entities have effective controls over expenditure using corporate purchasing cards.

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

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

CAROLINE SPENCER
AUDITOR GENERAL
27 March 2020

Contents

Executive summary 2

 Background 2

 Conclusion 2

 What we did 2

 Entities included in our audit..... 3

What we found..... 5

 Recommendations 7

Appendix 1: Better practice principles 9

Executive summary

Background

Western Australian government purchasing cards are an important part of the public sector purchasing system. Purchasing cards offer significant benefits to State government entities (entities), suppliers and the environment. They can reduce costs and streamline business processes associated with authorising, tracking, purchasing, payment and reconciling entity purchases and can also significantly reduce the use of paper.

However, if not managed correctly, there is potential for improper, wasteful or unauthorised expenditure. Entities need to ensure that appropriate controls are in place and be continually vigilant against misuse, and that the controls are assessed on a regular basis.

The use of WA government purchasing cards is governed by the *Financial Management Act 2006* and Treasurer's Instructions (TI) particularly TI 321 *Credit Cards – Authorised Use*.

We last reported an across government audit of State government purchasing cards in 2017. In that audit we identified a range of findings but concluded that there had been some improvement since our previous report in 2014.

Conclusion

Entities generally have appropriate policies and administrative systems in place to manage the use of purchasing cards. Although our findings indicate a general improvement in controls compared to our last report on this topic in 2017, we still identified examples of poor practice. Entities still need to improve their policies, the monitoring of purchasing card use, and better manage transaction limits.

What we did

The focus of our audit was to assess whether sampled entities have effective controls over expenditure using corporate purchasing cards, using the following criteria:

- Do entities have appropriate policies and administrative systems in place for government purchasing cards?
- Are suitable controls in place to monitor and manage the use of cards and the timely approval of transactions?
- Do entities periodically review their use of purchasing cards and act on any identified shortcomings?

As part of this audit, we used data analytics to review large volumes of transactions and data for unusual items, patterns and events that could indicate fraud. We then further investigated the transactions or events.

Detailed findings have been reported to audited entities. Entity audit committees should follow up to ensure the audit findings and recommendations are appropriately addressed by management in a timely manner.

We conducted this audit under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. The approximate cost of undertaking the audit and reporting is \$220,000.

Entities included in our audit

Focus area audits assess entities against common business practices to identify good practices, and control weaknesses and exposures so that all entities, including those not audited, can evaluate their own performance.

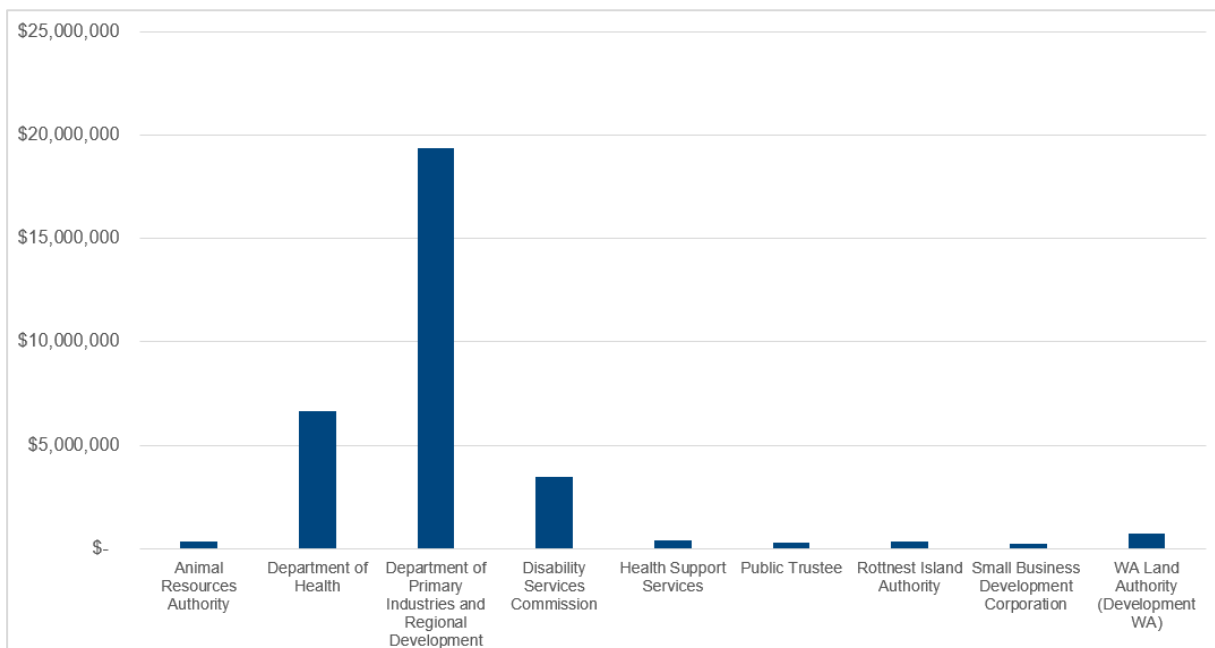
We selected a sample of 9 entities for this focus audit. When selecting the entities to be included, we considered the size of the entities and the different levels of purchasing card use to ensure that we were covering a wide variety in our sample.

Entity	Number of purchasing cards	Total purchasing card expenditure 1 July 2018 - 30 June 2019
Animal Resources Authority	8	\$317,772
Department of Health	111	\$6,662,154
Department of Primary Industries and Regional Development	1,022	\$19,361,424
Disability Services Commission	772	\$3,460,601
Health Support Services	47	\$395,034
Public Trustee	25	\$652,458
Rottnest Island Authority	62	\$362,440
Small Business Development Corporation	14	\$219,896
WA Land Authority (Development WA)	103	\$739,269

Source: OAG

Table 1: Entities included in our sample

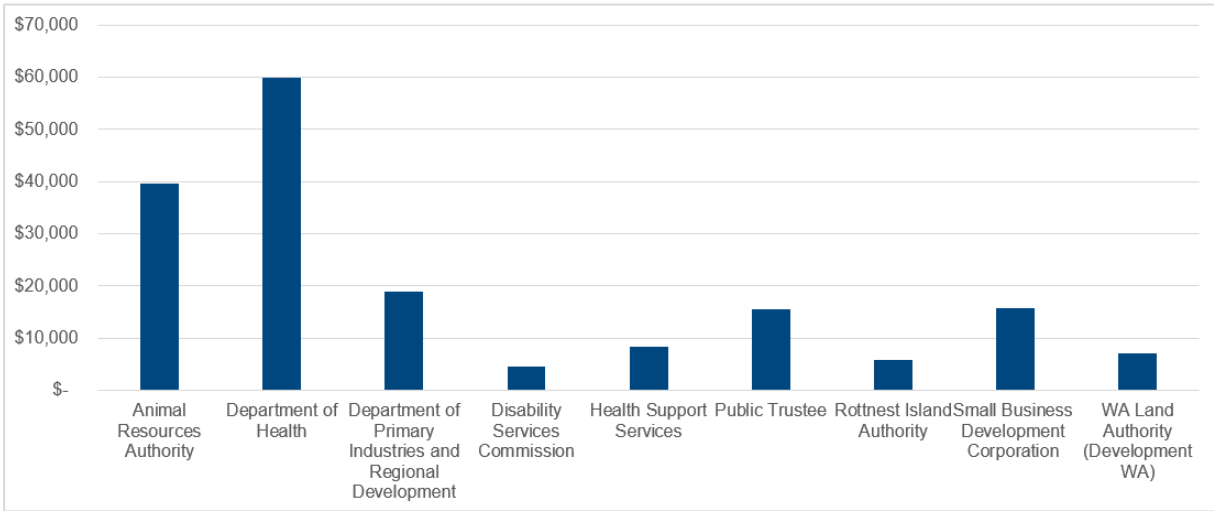
Figure 1 shows entities' total purchasing card expenditure during 2018-19 and Figure 2 shows the average spend on the purchasing cards we sampled.



Source: OAG

Figure 1: Total purchasing card spend per entity during 2018-19

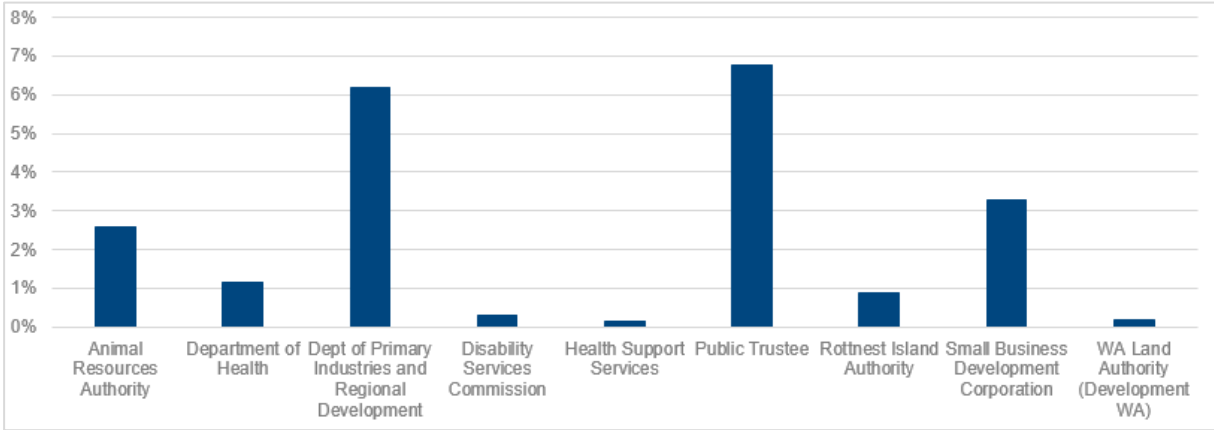
(Appendix AAR: 8.1B)



Source: OAG

Figure 2: Average spending on purchasing cards during 2018-19

Figure 3 shows the total purchasing card expenditure at the entities for the period 1 July 2018 to 30 June 2019 as a percentage of total expenditure.



Source: OAG

Figure 3: Purchasing card expenditure as a percentage of total expenditure

What we found

All entities had up to date and approved policies and procedures for the use of purchasing cards, however some aspects were not included

Good policies and procedures provide essential guidance for staff to manage purchasing cards in accordance with management's expectations. They should cover matters such as controls over issuing and cancelling cards as well as approving and acquitting purchases.

In 5 of the entities sampled, there was no policy or clarification regarding the return of cards while on extended leave. The policy should state what length of time represents extended leave and the need for the cardholder to return the card to the finance area while they are on leave.

Four of the entities also did not have a policy regarding the use of Paypal. Paypal can be an effective method of payment for certain purchases. However, its use creates an increased risk as the purchasing card is required to be linked to a Paypal account, which could result in the officer's personal expenses being recorded with the entity's transactions. If an entity uses Paypal, then it should have a more detailed policy on what can be purchased, and the type of evidence required for these purchases.

In 4 of the entities tested, the policy around hospitality and entertainment expenses needed to be clearer. Our data analytics testing noted a number of purchases in relation to food, gifts and alcohol. The policy at these entities is not clear on what is acceptable expenditure for hospitality, and delegated limits for these types of expenditure have not been set.

Most entities need to apply better controls over the use of cards

We tested a sample of 100 purchasing card transactions per entity and noted that a large number of them were supported by appropriate documentation, acquitted and approved in a timely manner, and were for business purposes. However, we still found a number of poor practices that had not been identified by the entities.

At 2 of the entities sampled, we noted instances where grocery store rewards program cards had been used when purchasing groceries. Public sector guidelines on gifts, benefits and hospitality require that purchasing cards should not be used to gain private advantage through the transaction. When rewards programs are used in conjunction with government purchasing cards, there is an increased risk of individuals making purchases through a particular supplier to gain a private advantage.

As part of our data analytics, we reviewed the purchasing card transactions to identify if expenditure on the card had occurred while the cardholder was on leave. Our testing identified that purchasing cards were being shared between staff at 5 of the entities sampled while the cardholder was on leave. One low value transaction was made when the cardholder was on leave, which was an allegedly fraudulent transaction that had not been reported. The risk of sharing a card is that an entity cannot hold a cardholder accountable for all of the transactions paid for using that card.

Our data analytics further identified instances of splitting payments at 3 entities. This occurs where the cardholder splits the payment of a transaction into 2 or more instances to circumvent the transaction limit set on the purchasing card. The risk of splitting a payment is that the cardholder is making a purchase at a value that they are not delegated to make.

We also found instances of personal use on purchasing cards in 3 of the entities where the cardholder did not notify the appropriate authority in a timely manner. We also noted a number of instances at these 3 entities where the money had not been repaid within 5 days of notification, as required by Treasurer's Instruction 321 *Credits Cards – Authorised Use*. If

(Appendix AAR: 8.1B)

personal use of a government purchasing card is not tightly controlled, it is possible that amounts may not be reimbursed.

Five entities had purchases that were not acquitted and approved in a timely manner

Of 600 transactions tested at 6 entities, 155 were not acquitted and approved in a timely manner (within 30 days). When transactions are not acquitted and approved in a timely manner, there is an increased risk that unauthorised transactions are not identified and resolved promptly.

We also noted that transaction limits were not applied to purchasing cards in 7 of the 9 entities sampled. The purchasing card system is set up to implement a transaction limit on cards, but these entities are not implementing or enforcing these limits. Not implementing a transaction limit increases the risk of a large monetary loss, as large inappropriate transactions can be processed in 1 transaction. For example, if a purchasing card has a \$100,000 limit with no transaction limit, the card holder could use the entire purchasing card limit in the 1 transaction.

None of the entities sampled had a formal review process to identify any shortcomings

Most of the entities sampled stated that they performed a periodic review of their purchasing cards, but none had formal records to evidence this.

From our review of the activity on purchasing cards across the 9 entities, we noted 475 cardholders who had used their purchasing card less than 12 times in the last 12 months, suggesting that they may not have a need for a purchasing card.

We also noted instances where business items were bought on the purchasing card that were outside the entity's purchasing card policy, for example, the purchase of IT equipment and fuel.

Regular formal reviews would identify similar issues in a timely manner, and enable an entity to take appropriate corrective action, including training for card users.

Recommendations

All entities should:

1. have appropriate policies and administrative systems in place for the use of government purchasing cards
2. ensure that they have suitable controls in place to monitor and manage the issue and use of cards and the timely approval of card transactions
3. periodically review the use of purchasing cards within the entity to identify and act on any shortcomings, such as whether there are too many cards within the entity, or that they are not being utilised to their full advantage.

Response from State government entities

Entities in our sample generally accepted the recommendations and confirmed that, where relevant, they have amended policies and administrative systems, or will improve practices for managing purchasing cards.

Appendix 1: Better practice principles

The following table shows control principles on which our audit focused. They are not intended to be an exhaustive list.

Controls over purchasing cards	Focus area	What we expected to see
Policy	Policies and procedures	<ul style="list-style-type: none">• Entities should have a purchasing card policy that is up to date and accessible to all staff. The policy should include items such as:<ul style="list-style-type: none">○ processes and controls for the issue, management and cancellation of a credit card, including credit card limits, validation and acquittal of expenditure○ purposes for which a card may, or may not, be used○ cardholder's obligations (including during leave periods)○ processes for discharging any debt for personal expenditure on a credit card○ process for online purchases, including Paypal.
	Delegations	<ul style="list-style-type: none">• There are appropriate delegations in place for monetary limits on cards, monitoring the use of purchasing cards and approval of expenditure.• Where appropriate, delegations should also be set for certain types of expenditure.
Use of purchasing cards	Managing and monitoring the use of cards	<ul style="list-style-type: none">• All purchasing card transactions should be valid, properly incurred, certified and accounted for in accordance with the entity's purchasing card policies.• New cards should be properly authorised before use.• Cancelled cards should be cancelled on a timely basis to ensure unauthorised transactions do not occur.• When employees go on leave, purchasing cards should be returned to the Card Administrator or another approved officer, and not shared with other employees.• All transactions should be within the delegated transaction limits and transactions should not be split to circumvent these limits.
Monitoring of purchasing cards	Appointment of a reviewer	<ul style="list-style-type: none">• The entity should have an appointed reviewer as required by TI 321.• A review of purchasing cards should be carried out on a regular basis and evidence of the review should be retained.• Management should periodically review credit card activity to identify inactive or under-used cards that may warrant cancellation.

Source: OAG

(Appendix AAR: 8.1B)

Auditor General's reports

Report number	2019-20 reports	Date tabled
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

 @OAG_WA

 Office of the Auditor General for
Western Australia

Western Australian Auditor General's Report



Local Government Contract Extensions and Variations and Ministerial Notice Not Required

Office of the Auditor General Western Australia

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

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

© 2020 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Local Government Contract Extensions and
Variations
and
Ministerial Notice
Not Required**

Report 20: 2019-20
May 2020



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

**LOCAL GOVERNMENT CONTRACT EXTENSIONS AND VARIATIONS AND
MINISTERIAL NOTICE NOT REQUIRED**

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

This focus area audit assessed if entities adequately managed extensions and variations to their contracts, and if they maintained comprehensive summaries of their contracts.

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

Also included is my determination that a section 82 notice was not required by the Minister for Water.

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

CAROLINE SPENCER
AUDITOR GENERAL
4 May 2020

Contents

Local government contract extensions and variations..... 2

Executive summary 2

 Background 2

 Conclusion 2

 What we did 2

What we found..... 4

 Recommendations 8

 Response from entities..... 8

Appendix 1: Better practice principles 9

Ministerial notice not required 12

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Local Government Contract Extensions and
Variations**

Executive summary

Background

Western Australia's 148 local government entities (entities) spend billions of dollars each year on purchasing a wide range of goods and services. A significant number of these purchases involve contracts.

Procurement contracts vary in complexity, value, duration and risk, but all benefit from a strong approach to contract management. Robust contract management processes centred around the principles of probity, accountability and transparency help to ensure that contracting is effective, meets the standards expected by the community and the Parliament and provides good value for money for the ratepayer.

Comprehensive policies and good management of contract extensions and variations are essential to achieving these outcomes. It is important for all entities to maintain a summary of their contracts in a register or database (hereafter referred to as register), with all key contract details, to help effectively manage contract extensions and variations. This is essential from an accountability perspective and also assists entities in meeting their financial reporting obligations.

Conclusion

At 5 entities there was insufficient documentation to demonstrate that extensions or variations were given due consideration, so we were unable to conclude if they were appropriately managed. At 3 entities, some extensions did not have evidence of contractor performance reviews, and at 3 entities some variations were not approved by delegated officers.

Most entities need to enhance their policies with comprehensive guidance. All entities' contract registers lacked key information essential to effective monitoring of contractual obligations.

What we did

The focus of this audit was to assess if entities adequately managed extensions and variations to their contracts, and if they maintained comprehensive summaries of their contracts.

We assessed the policies, procedures and practices for managing contract extensions and variations at 8 entities of varying sizes in both metropolitan and regional Western Australia. We assessed the following criteria:

- Do entities have adequate policies and procedures for managing contract extensions and variations?
- Do entities have complete and accurate summaries of their contracts?
- Are entities adequately:
 - controlling contract extensions, including the review of contractor performance before extending contracts
 - controlling contract variations, and determining if a variation significantly changes the original scope of the contract
 - complying with management approved delegations before a contract is extended or varied?

(Appendix AAR: 8.1C)

When testing against these criteria, we had regard for Part 4 of the Local Government (Functions and General) Regulations 1996, which deals with the provision of goods and services, and includes specific requirements relating to contract extensions and variations. In addition, we expected entities to meet the principles of the *Local Government Act 1995*, which requires entities to have policies, and to keep proper accounts and records. We also had regard to the broader principles of good internal control and governance and general better practice principles that help reduce procurement risks and support value for money.

The audit focused on whether controls were in place to support effective management of contract extensions and variations after a contract was finalised. It was not designed to review the adequacy of procurement processes undertaken prior to the signing of the original contracts.

The following 8 entities were included in this audit:

Entities
City of Bayswater (Bayswater)
City of Kwinana (Kwinana)
City of Rockingham (Rockingham)
City of Swan (Swan)
Shire of Narrogin (Narrogin)
Shire of Wagin (Wagin)
South Metropolitan Regional Council (SMRC)
Town of Cottesloe (Cottesloe)

Source: OAG

Table 1: Entities included in the audit

We assessed contract extensions and variations processed from 1 January 2018 to the date of the audits, in mid-2019.

Detailed findings have been reported to audited entities. Their audit committees should follow up to ensure audit findings and recommendations are appropriately addressed by management in a timely manner.

We conducted this audit under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. The approximate cost of undertaking the audit and reporting was \$177,500.

What we found

The contract management policies and procedures at most entities lacked appropriate guidance for staff to correctly and consistently process extensions and variations. We also found contract registers at all 8 entities were missing key information required for effective contract management.

We found instances at 5 entities where sound practices were not always followed for assessment and approval of extensions and/or variations. We therefore could not conclude whether this represented probity in purchasing and value for money for the ratepayer.

Policies and procedures need to be enhanced to ensure consistent application by staff

Comprehensive policies and procedures provide clear guidance to staff, help ensure that regulatory requirements are complied with, and that better practices are consistently followed by all staff. It is also important to have clear documentation of delegated authorisations to ensure that all decisions on contract extensions and variations are made by officers within their delegated authority limits.

Kwinana had sound policies and procedures for managing contract extensions and variations, with scope for improvement at the other 7 entities.

We identified the following shortcomings:

- Four entities did not have clearly established authorisations and delegations for the approval of contract extensions and/or variations. Establishing clear lines of responsibility and accountability for all decision making is an important prerequisite to ensuring decisions are made by individuals the entity considers have the requisite skills, knowledge and experience.
- The policies of 5 entities lacked guidance on what constitutes an appropriate contract variation. For example, a contract variation to provide goods and services that is inconsistent with the scope of the original contract, or significantly alters the scope of the original contract is not appropriate. In such circumstances, a separate procurement process would normally be required.
- The policies of 6 entities did not outline the key requirements for processing contract extensions, including that contracts could be extended only if the terms of the original contract included extension options.
- The policies or procedures of 5 entities did not require a documented performance assessment of a contractor before a contract extension option was considered. This increases the risk that poor performing contractors may be granted extensions.
- No entities' policies or procedures required staff to maintain a contract register, with all key contract information.
- Six entities did not require a regular review of their contract registers to identify contracts that are due to expire, so that appropriate action starts well before the contract expiry date. Lack of a review process increases the risk that contract extension decisions may be rushed, leading to inappropriate extensions, and potentially impact continuity in the provision of goods and services.

Contract registers did not include key information for effective contract oversight

It is important for all entities to maintain a summary of their contracts, with all key information, to help contract managers effectively manage contract extensions and variations.

The entities in our audit maintained records of their contracts on databases, registers, or a combination of both. One entity did not have any collective record of their contracts at the commencement of the audit, but subsequently provided us with a contract summary. The contract registers at the 8 entities did not include all key contract information. We identified the following:

- The contract registers at 2 entities were incomplete and did not include all current contracts. The register at another entity did not include the commencement, duration and end dates of contracts. A fourth entity's register included inaccurate and/or inconsistent information on key data such as contract values, term dates and the status of contracts. Inaccurate and incomplete contract registers can affect management's ability to effectively manage contracts.
- At 6 entities, the contract registers did not include the dollar value of contracts, or any contract extensions or variations. In addition, at 3 of these entities, registers did not include the estimated dollar value of Schedule of Rate¹ contracts. As a result, inadequate information was available to management on the total cost of their contracts.
- Where relevant, although details of contract variations are contained within individual contract management plans, none of the entities' contract registers included summarised information on approved contract variations, such as the number and dollar value of individual variations, and the total value of approved variations. This information is essential for contract managers to effectively track the cumulative value of contract variations, evaluate the impact on the scope of the original contracts, and initiate separate procurement processes where appropriate.
- At 4 entities, contract registers did not include information on the number and duration of extension options available under each contract and details of extension options that were exercised. This information would enable better monitoring of contracts, including the timely exercise of contract extension options.
- The contract registers at 6 entities did not have details of scheduled performance review dates, to ensure that timely reviews of contractor performance were performed prior to considering contract extension options.

Some entities need to improve their assessment of contractors' performance before extending contracts

A contract extension may extend the agreed terms for a further period and/or involve changes to price, personnel and services. We expected to find evidence that contract managers had performed an adequate and timely review of contractors' performance before granting an extension. This would provide management with adequate opportunity to assess if the contractor still offered value for money.

¹ Schedule of Rates contracts are used where the nature of contract work is certain, but the exact amount of work to be performed cannot be predicted at the outset and is inherently provisional in nature. Nonetheless, tenders are usually invited and awarded based on the range of estimated quantities.

(Appendix AAR: 8.1C)

All entities except Rockingham and Kwinana exercised contract extension options during our audit period. One of the 6 did not have detailed records of the total number and value of contract extension options exercised. Based on the contract registers of the remaining 5 entities, 51 contract extension options totalling \$19.6 million were exercised during the audit period.

We tested a sample of 18 contract extensions totalling \$13.6 million across the 6 entities. Narrogin, Wagin and SMRC had adequate processes in place for the extension of contracts.

At the other 3 entities, we noted the following shortcomings:

- At 2 entities, 6 of 7 contract extensions did not have any formal documentation to demonstrate that an assessment of contractor performance was conducted before the contract extensions were approved. We were therefore unable to conclude if there was adequate review of contractor performance before exercising the extension options. This increases the risk that poor performing contractors may be granted extensions. The total value of 5 of these extensions was \$1.4 million, while the value of the remaining extension could not be determined as the original contract was not available.
- Three extensions at 2 entities totalling \$1.48 million were approved after the expiry of the initial contracts. One of the entities advised that there were extenuating circumstances that resulted in a short period when some key functions were performed later than usual. Renewal processes that are not initiated well before the expiry of contracts, limit the entities' ability to assess whether the contracts still offer the best value for money. This also potentially impacts the continued supply of goods and services.
- For 2 of 5 contract extensions at 1 entity, there was no mutually accepted agreement or correspondence between both the parties to extend the contract.

Contract variations were not always adequately explained at 2 entities

Contract variations are amendments to a contract that change the original terms or conditions. Variations are usually used to alter the scope of the supply or services provided or to change pricing. We considered if contract variations, individually or cumulatively, significantly altered the scope of the original contract. This may indicate that an entity was using variations to avoid undertaking a new procurement process.

All entities except Wagin undertook contract variations during the period of our audit, although only 5 were able to provide detailed information of the total number and value of their contract variations processed. The contract registers of these 5 entities showed 63 variations totalling \$6 million. We reviewed 27 contract variations totalling \$5.2 million across the 7 entities.

At 2 entities, 4 of 12 variations were not supported by detailed proposals with descriptions of the nature and reasons for the variations, including associated cost, time and scope implications. We were therefore unable to conclude whether the variations had been approved based on adequate analysis of these implications and whether value for money assessments had been performed.

Delegation levels were not always complied with when extending or varying contracts

It is important that all decisions relating to the approval of contract extensions and variations are made in accordance with approved authorisation limits. This ensures that these decisions are valid, and are made by staff with the experience and knowledge commensurate with the value and complexity of the contracts involved.

8.2B

(Appendix AAR: 8.1C)

We reviewed the approval processes of 27 variations valued at \$5.2 million and 18 contract extensions totalling \$13.6 million across all 8 entities and identified the following shortcomings:

- At 2 entities, 7 variations totalling \$1.2 million were approved by officers in excess of their delegated authority.
- At a third entity, we identified 2 variations to a contract totalling \$77,395 that significantly changed the scope of the original contract, increasing the contract value in excess of the \$150,000 tender threshold limit. The consequent waiver from tender was approved by an officer who did not have the delegated authority.
- Two extensions totalling \$73,058 at 1 entity did not have any documented evidence of their approval. We were therefore unable to conclude if an appropriate officer had approved them. This reduces transparency and accountability in decision making and increases the risk that the mandated level of scrutiny is not applied.

Recommendations

1. All local government entities, including those not sampled in this audit, should:
 - a. ensure their policies and procedures include comprehensive guidance to staff on recording of contract information and management of contract extensions and variations, so that better practices are consistently applied across the organisation
 - b. establish specific delegated authorisation limits for the approval of contract extensions and variations
 - c. ensure their contract summaries include all key information relating to contracts. The level of information should be based on their assessment of the significance, number and complexity of their contractual arrangements
 - d. ensure that records of key decisions are retained in accordance with their recordkeeping plans and are readily available
 - e. improve review processes relating to contract extensions, including timely and documented reviews of contractor performance before exercising contract extension options
 - f. ensure that contract variations are supported by adequate documentation describing the nature and reasons for the variations, including the associated cost, time and scope implications. The cumulative impact of variations on a contract should also be reviewed and an assessment made of whether a separate procurement process should be undertaken
 - g. ensure that all contract extensions and variations are approved in accordance with approved delegations, to ensure that all contracting decisions are subject to appropriate levels of scrutiny.
2. Entities should review their policies and procedures against the principles in Appendix 1.

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

Response from entities

Entities in our sample generally accepted the recommendations and confirmed that, where relevant, they have amended policies and administrative systems, or will improve practices for managing contract extensions and variations.

Appendix 1: Better practice principles

The following table shows control principles on which our audit focused. They are not intended to be an exhaustive list.

Management of contract extensions and variations	Focus area	What we expected to see
Policy	Policies and procedures	<ul style="list-style-type: none">• Contract management policies and procedures are regularly reviewed to ensure compliance with current legislation and relevance to current operations.• Policies or procedures include a requirement to maintain a comprehensive register or database of all contracts, including:<ul style="list-style-type: none">○ the dollar value above which contracts are to be included in the register, and○ the custodian of the register with responsibility for regular review and update of the contract register or database.• Policies include clear guidance on what constitutes a contract variation and when a separate procurement process is required.• The policies or procedures provide guidance on the key processes for contract extensions, including timely and documented assessments of contractor performance prior to exercising an extension option.
	Delegations	<ul style="list-style-type: none">• There are appropriate delegations and authorisations in place for procurement as well as for contract extensions and variations.
Records	Comprehensive register of contracts	<ul style="list-style-type: none">• A comprehensive register of all contracts is maintained, with all key contract information.
Contract extensions	Contract terms	<ul style="list-style-type: none">• Contracts are extended only if the original contract includes extension options.
	Approval	<ul style="list-style-type: none">• Contract extensions are approved by an appropriate officer, in accordance with delegated authorisation limits.• Extensions are approved before the expiration date of the original contract or previously extended term, for continuity in the provision of services.
	Contractor performance review	<ul style="list-style-type: none">• There is documented evidence that contractor performance has been assessed before a contract extension is approved.

(Appendix AAR: 8.1C)

Management of contract extensions and variations	Focus area	What we expected to see
	Recordkeeping	<ul style="list-style-type: none">• There is documented evidence that the terms of the contract extension have been mutually agreed by the entity and the contractor.• Documents for approval of contract extensions are retained in accordance with recordkeeping plans, to promote accountability and transparency in decision making.
Contract variations	Approval	<ul style="list-style-type: none">• Contract variations are approved by an appropriate officer, in accordance with delegated authorisation limits.• Consideration is given to the cumulative impact of variations, to ensure that the scope of the original contract is not significantly altered, and that a separate procurement process is not required.
	Proposal for variation	<ul style="list-style-type: none">• Contract variations are supported by proposals with detailed description of the nature of the variation, with associated cost, time and scope implications.
	Recordkeeping	<ul style="list-style-type: none">• The variation proposals and approval documents are retained in accordance with recordkeeping plans, to promote accountability and transparency in decision making.

Source: OAG

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Ministerial Notice Not Required

Ministerial notice not required

On 24 March 2020, we received 2 notices from the Minister for Water, the Hon David Kelly MLA, under section 82 of the *Financial Management Act 2006* (FMA) in relation to Legislative Assembly Questions on Notice 5872 part (6) and 5873 part (c).

On 10 December 2019, the Hon Terry Redman MLA asked the Minister for the following information:

Legislative Assembly Question on Notice 5872

(1) I refer to the recent Freedom of Information (FOI) released by Water Corporation including a redacted copy of "PRA Business Case" arguing the value of "insourcing the Perth Region Alliance", and ask?

(6) Will the Minister table a copy of the "Alliance Agreement" referenced on page 10 of the business case?

On 19 March 2020, the Minister replied:

(6) The Alliance Agreement is a commercial contract arrangement between the Water Corporation and Programmed Facilities Management.

Legislative Assembly Question on Notice 5873

I refer to the decision by Water Corporation to insource the services currently provided under the Aroona Alliance, and ask:

(c) Can the Minister table the Aroona Alliance contract;

On 10 March 2020, the Minister replied:

(c) The Alliance Agreement is a commercial contract arrangement between the Water Corporation and the Alliance partners.

The Minister's notices advised that the Perth Regional Alliance Agreement and the Aroona Alliance Contract could not be provided to Parliament, as their release would disclose commercially confidential and sensitive information.

We determined that the 2 notices were not required in this instance, as the information does not concern the conduct or operation of an agency as required by the FMA. Section 85 of the *Water Corporations Act 1995* outlines the limited application of the FMA and the *Auditor General Act 2006* to the Water Corporation, but this does not cover section 82 of the FMA.

The Audit Practice Statement on our website (www.audit.wa.gov.au) outlines the circumstances when a notice is unlikely to be required. These include when the requested information does not concern the conduct or operation of an agency as required by the FMA.

Auditor General's reports

Report number	2019-20 reports	Date tabled
19	Control of Monies Held for Specific Purposes	30 April 2020
18	Information Systems Audit Report 2020 – State Government Entities	6 April 2020
17	Controls Over Purchasing Cards	27 March 2020
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

 @OAG_WA

 Office of the Auditor General for
Western Australia

Western Australian Auditor General's Report



Western Australian Public Sector Audit Committees – Better Practice Guide

Office of the Auditor General
Western Australia

Report team:

Jordan Langford-Smith
Mona Loo
Jo Stapley
Vanessa Kar
Financial Audit Directors

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

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

© 2020 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISSN: 2200-1913 (Print)
ISSN: 2200-1921 (Online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Western Australian Public Sector Audit
Committees – Better Practice Guide**



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

**WESTERN AUSTRALIAN PUBLIC SECTOR AUDIT COMMITTEES – 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 first comprehensive stand-alone better practice guide we have produced.

While prepared primarily as a resource for audit committees in State and local government entities, it also provides Parliament with further insight on the significant role public sector audit committees play in supporting quality public administration.

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

CAROLINE SPENCER
AUDITOR GENERAL
25 June 2020

Contents

Auditor General’s overview.....	4
Part 1: Introduction	5
1.1 About this guide.....	5
1.2 Who should use this guide	6
1.3 Lines of defence model	7
1.4 Acknowledgements	8
Part 2: Key challenges to building effective audit committees.....	9
2.1 Establishing and maintaining effective relationships between the three governance parties	9
2.2 Getting the right balance of skills and experience.....	11
2.3 Enabling robust discussions at audit committee meetings	13
2.4 Being aware of all assurance activities	14
2.5 Seeking assurance on organisational culture	15
Part 3: Principles for better practice audit committees.....	18
Part 4: Guidance for audit committee fees.....	24
Part 5: Guidance for smaller entities.....	25
Part 6: Toolkit	27
Tool 1 Example audit committee charter	28
Tool 2 Audit committee member induction checklist	37
Tool 3 Meeting preparation checklist.....	39
Tool 4 Meeting agenda template	41
Tool 5 Characteristics of effective meetings	43
Tool 6 Annual work plan template	44
Tool 7 Audit recommendations progress report template	49
Tool 8 Review of OAG audit reports template.....	50

Auditor General's overview

Audit committees play a fundamental role in assisting directors general, councils and boards to fulfil their governance and oversight responsibilities. They are not a substitute for good management and controls. Instead, they help provide advice and independent assurance to the accountable authority on how effective these controls are.



The purpose of this guide is to provide better practice principles and guidance to accountable authorities, audit committee members and senior managers with responsibility for audit committee activities. We have drawn from our experience in interacting with audit committees at State and local government entities, as well as guidance from the Institute of Internal Auditors and other jurisdictions.

WA public sector entities range in size and complexity. Service delivery, rigorous compliance requirements and the ability to attract and retain skilled, qualified and experienced staff can be a challenge. To assist smaller entities to address these challenges, we have included some specific guidance to help them implement simple, yet effective practices to strengthen the effectiveness of their audit committees. There is also a toolkit in part 6 of the guide with useful resources for all entities.

Maintaining a strong ethical organisational culture is important in promoting excellence and efficiency in public service delivery, as well as minimising the risk of fraud and corruption. Failures in governance and integrity are all too common across sectors and jurisdictions, and recent inquiries into the finance sector have highlighted the important role that audit committees play in challenging management and holding them accountable. Poorly governed entities often have common characteristics, including a lack of an accountability culture that can be evident in such areas as long overdue internal and external audit recommendations. By ensuring that management promptly address weaknesses identified in internal and external audits, and by rigorously overseeing internal audit, risk management and compliance functions, audit committees can help to establish the right tone and culture within entities.

The guide provides principle-based guidance for State and local government entities in Western Australia. We recognise that the specific legislative and regulatory requirements for State and local government entities are different, and it is therefore difficult to have a 'one-size-fits-all' approach for better practice guidance. Entities need to consider their relevant legal and regulatory requirements as well as operating environment when using this guide.

It has been pleasing that the importance of public sector audit committees has been elevated recently, which included the introduction of a revised Treasurer's instruction for audit committees in State government entities. While our guide is not mandatory or intended to be a prescriptive list of requirements, I hope that it serves as a useful resource for entities in assessing and improving their audit committees for the benefit of the Western Australian community.

Part 1: Introduction

Audit committees are an essential part of an entity's governance framework. They provide independent advice and assurance to accountable authorities on systems of risk management and internal control, and financial and performance reporting. (Figure 1).

All State and local government entities in Western Australia are required to establish an audit committee that is independent from management influence, a fundamental element of effective audit committees. If they are not independent, objectivity may be compromised, making it difficult for them to perform their oversight roles.



Source: OAG

Figure 1: Scope of audit committee oversight responsibilities

1.1 About this guide

This guide provides better practice principles and guidance on common key challenges that audit committees face.

The guide consists of six parts:

Part 1: Introduction outlines the purpose of the guide and explains the lines of defence model.

Part 2: Key challenges to building effective audit committees provides insight into the key challenges faced by audit committees based on our observations from attending a wide range of Western Australian public sector audit committees.

Part 3: Principles for better practice audit committees outlines core better practice principles for our State public sector audit committees based on guidance from the Institute of Internal Auditors Australia (the IIA). These principles are as follows:

Principles for Better Practice Audit Committees	
1.	Membership: Members have the right experience and leadership skills to be trusted independent advisors.
2.	Role and Responsibilities: The roles and responsibilities of the audit committee allow for wholesome oversight of internal audit, governance, risk management and internal control practices.
3.	Professional Practices: The audit committee conducts itself professionally to provide independent, sound and valuable advice to the accountable authority.
4.	Performance and Accountability: The audit committee is aligned with the entity's strategic outcomes and is accountable for its performance.
5.	Entity Relationships: The audit committee is a trusted, independent partner.
6.	Governance and Reporting: The audit committee is governed effectively to enable transparent, objective and timely reporting.

Part 4: Guidance for audit committee fees outlines information to guide fee arrangements for external audit committee members.

Part 5: Guidance for smaller entities provides practical measures that smaller entities could apply to build effective audit committees with limited resources.

Part 6: Toolkit includes a comprehensive compilation of templates and checklists which can be used to help develop effective audit committees.

Throughout the guide, we have used the term 'accountable authority' to collectively represent:

- for State government entities, the Director General, Commissioner, Board, or other person responsible for the direction and control of the entity as defined in the *Financial Management Act 2006* or relevant legislation
- for local government entities, Councils. This reflects the direct reporting relationship between the audit committee and Council under the *Local Government Act 1995*. However, it is important to note that the Chief Executive Officer (CEO) has some responsibilities under the Act, including financial reporting, which instead rests with the accountable authority in State government entities.

We have also used the term 'audit committee' to represent all public sector audit-related committees. Within the public sector, there is a wide range of names for audit committees, such as, Audit and Risk Committees.

1.2 Who should use this guide

While we have tailored this guide for public sector entities in Western Australia, the principles and practices outlined in this guide generally apply to all audit committees.

This guide is suitable for members of audit committees, accountable authorities, CEOs, chief audit executives and senior managers with responsibility for audit committee activities, as well as those who are accountable to an audit committee.

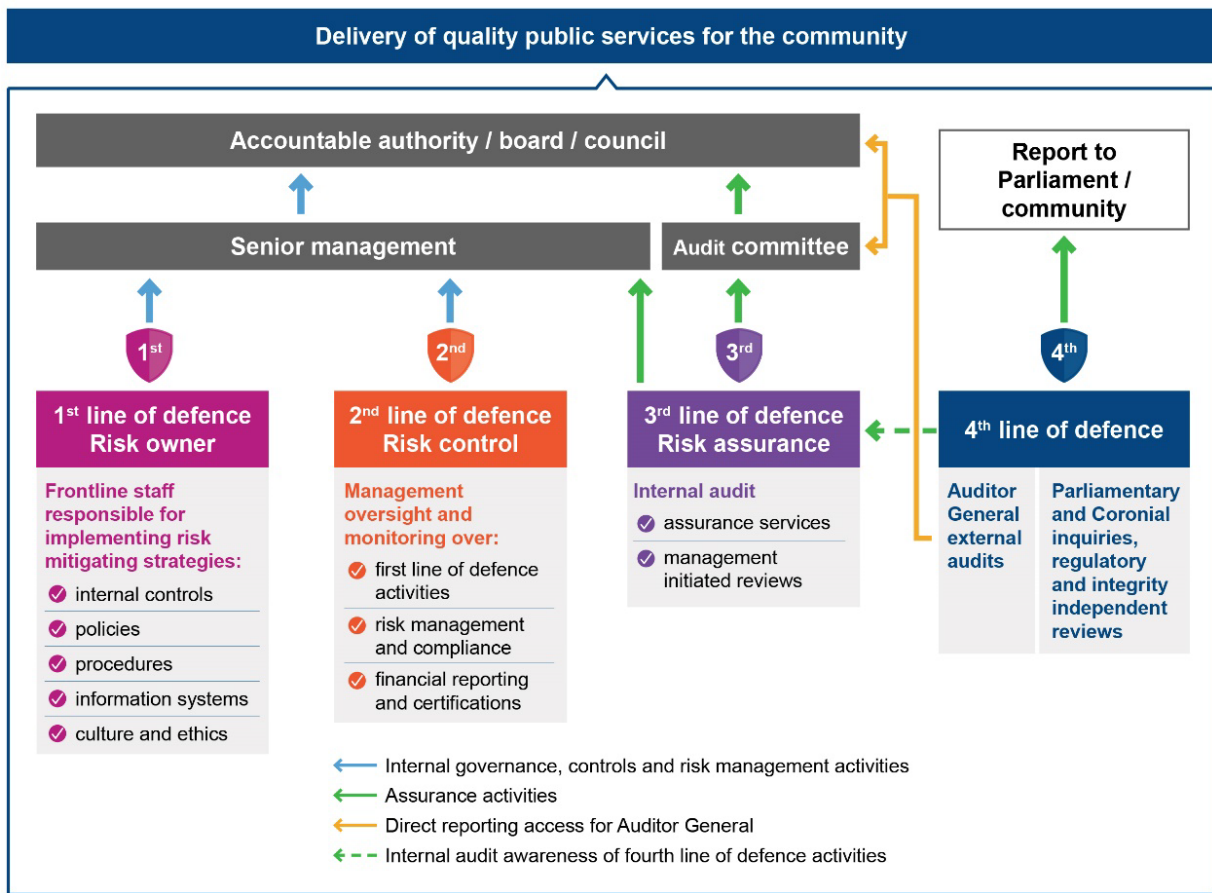
1.3 Lines of defence model

The lines of defence model is a visual representation of the different mechanisms (defences) which all work together to manage risks and ensure that controls are implemented and effective. It helps to provide a coordinated approach for managing entities' risks.

All entities regardless of their size and complexity should establish a good understanding of their risks and four lines of defence.

The lines of defence model typically identifies the 3 lines of defence within the entity. However, external auditors, regulators, parliamentary committees and other integrity bodies also provide important information and assurance on the implementation of controls within an entity. We have referred to these entities as the fourth line of defence.

Figure 2 below illustrates the activities for each line of defence and the general flow of communication between each of the bodies.



Source: OAG

Figure 2: WA public sector four lines of defence model

To apply the model, entities need to understand and assess business activities performed by each line of defence. This is often referred to as 'assurance mapping'. This mapping helps the accountable authority, audit committee and management to understand whether there are any gaps in assurance activities that manage key risks or whether there is duplication of effort. This can help inform the internal audit program, improve efficiency and assist the audit committee in their oversight responsibilities.

1.4 Acknowledgements

We would like to express our appreciation to the public sector entities and their staff and individual audit committee members and Chairs for sharing their valuable insights. In particular, a number of stakeholders, experienced in governance and accountability roles, willingly shared their views and suggestions for this guide. We highly valued and appreciated their input, guidance, advice and time.

In addition, we would like to thank the Institute of Internal Auditors - Australia (and Global) and the Australian National Audit Office who allowed us to use their resources to inform our guide.

Part 2: Key challenges to building effective audit committees

2.1 Establishing and maintaining effective relationships between the three governance parties

High functioning audit committees rely on strong working relationships between the accountable authority, the head of internal audit (the chief audit executive) and the audit committee (Figure 3). To support effective governance of an entity, the communication between them needs to be open, transparent and built on a relationship of trust.

Source: OAG

Figure 3: Relationships between the three governance parties



Roles and responsibilities of governance parties

Accountable Authority is responsible for establishing an effective audit committee and internal audit function¹ which is suitable for the entity. The accountable authority relies on the audit committee to provide independent oversight over the governance of financial and non-financial activities.

Chief Audit Executive is the head of internal audit within an entity. To maintain their independence, the Chief Audit Executive (CAE) should not perform key management duties. For example, the Chief Finance Officer should not take on the role of CAE.

For local government entities, responsibility for the internal audit function rests with the CEO, who also reports to the audit committee and council. Given that it is important for internal audit to be independent from management, it is good practice for the CAE to also have a direct line of communication to the audit committee (a functional reporting relationship).

To be effective, the Chief Audit Executive needs to be of a sufficiently senior level and respected by management as a key contributor to good governance and entity outcomes. This means that they need to be aware of current initiatives and activities within the entity, be suitably qualified, have open access to senior management and the accountable authority and adequate resources to carry out internal audits and support the audit committee.

While entities can use different models for their internal audit services (in-house, co-sourced or fully outsourced), it is critical that the entity appoint a CAE who is responsible for the internal audit function. This role should be performed by a capable and respected professional internal to the entity, even if all internal audit services are outsourced. The roles and responsibilities of the CAE should be documented and formally approved in the Internal Audit Charter.

Audit Committee provides independent advice and assurance to the accountable authority over the entity's systems of risk management and internal control, and financial and performance reporting. It consists of a group of members who support the accountable authority to instil strong control and risk practices within the entity by overseeing and probing

¹ For State entities only, refer to section 53(1)(d) of the *Financial Management Act 2006*.

(Appendix AAR: 8.1D)

activities relating to governance, control, risk management and compliance. The audit committee does not, and should not, hold formal decision-making powers. Rather, it relies on the skills and expertise of members to obtain sufficient appropriate information, through the CAE and internal auditors as their “eyes and ears”, as well as reports from management and external auditors and advisers.

For local government entities, the role of audit committee is prescribed by the *Local Government Act 1995* and *Local Government (Audit) Regulations 1996*. They do not have powers or authority to implement actions in areas over which the CEO has legislated responsibility and they do not have any delegated financial responsibility. The committee does not have management functions and cannot involve itself in management processes or procedures.

Key aspects for effective relationships between the governance parties

Supporting the independence of the CAE

The accountable authority and audit committee must take an active role in promoting the independence of internal audit and protect them from pressure from senior management. There are some cases where the accountable authority and audit committee need to increase their support for the CAE. For example, if management seeks to limit internal audit activities and scope, takes an overly defensive attitude towards audit findings, attacks the credibility of the CAE or fails to respond to audit enquiries and recommendations.

The audit committee needs to receive and request the right information

The audit committee may struggle to effectively perform its duties if it does not receive or request the right information. The committee needs to know what information to “pull” from internal audit and the CAE needs to know what information to “push” forward to the audit committee. To establish this flow of information, there must be strong working relationships between the audit committee and CAE and an understanding of what information both parties need.

It is important that the audit committee and CAE are clear about the expectations of internal audit. Having clear expectations about the content, format and frequency of internal audit reports and other reporting is crucial to having an effective relationship.

A good example of this is the CAE and audit committee Chair working effectively together, where possible, to establish an agenda for the audit committee meeting. The agenda should not be set by one party in isolation. Instead, the Chair needs to be comfortable obtaining information from the CAE to inform and direct the meeting. Similarly, the CAE needs to be confident in raising matters or concerns with the Chair and helping to guide the agenda and discussions.

Figure 4 provides some practical examples of common challenges faced by entities and how the 3 governance parties can work together to overcome the challenge.

Better practice activity	Example scenario
Timely and open engagement with the audit committee on an emerging issue	The entity is subject to a cybersecurity attack and activates its incident response plan. As part of the response, senior management writes to the Chair of the audit committee to inform them of the breach and to seek their input on management’s planned response. At the next audit committee meeting, management provides an update on the incident and key decisions and outcomes agreed by management as part of their regular reporting on cybersecurity incidents. The audit committee evaluates risk management actions and internal audit plans based on this information.

Better practice activity	Example scenario
	The timely and open discussion at the audit committee meeting provides additional independent assurance to the accountable authority that the measures the entity took to address the major incident are sound and based on informed decisions.
Treating the CAE as a trusted partner	<p>A senior executive decided not to implement recommendations from an internal audit on project management because the project was completed. The senior executive sought the accountable authority's approval to close the recommendations, without seeking input from the CAE.</p> <p>The accountable authority then checked whether the CAE was consulted on the decision. When the accountable authority became aware that the CAE was not consulted, the accountable authority sought advice from the CAE prior to deciding on the matter. The accountable authority reminded senior executives of the need to engage with the CAE when considering internal audit recommendations.</p>
CAE reporting directly to the audit committee and accountable authority	<p>The CAE administratively reported to a senior executive who was trying to limit the scope of an internal audit in the executive's area, without informing the audit committee.</p> <p>The CAE reminded the senior executive that they also need to report to the accountable authority and audit committee. The CAE raised the matter with the Chair of the audit committee and accountable authority and sought their advice. The accountable authority informed the executive team about the independence of internal audit, and allowed the CAE and audit committee to determine the scope of the internal audit to obtain the necessary assurance on priority risks.</p>

Source: OAG

Figure 4: Examples of effective relationships between the governance parties

2.2 Getting the right balance of skills and experience

It is essential that audit committee members have the right experience, personal qualities and independence to effectively perform their duties.

Independence is key

Having independent audit committee members who are free from management oversight and responsibility will help to bring an objective perspective and fresh insights to audit committee discussions. Audit committees that fully or predominately consist of senior management members will have difficulties in setting aside their management responsibilities to perform their oversight role. While local government entities and statutory authorities have a natural division between those charged with governance and management, this is not the case for State government departments.

Changes to Treasurer's Instruction 1201: 'Internal Audit' (TI 1201), in 2019 have strengthened the independence of audit committees. All State government entities subject to the Treasurer's instructions are required to have an audit committee Chair who is not employed by the entity and is suitably qualified. The guidelines in TI 1201 also recommend having a majority of members who are free of management responsibility and oversight.

For local government entities and statutory authorities whose audit committee members comprise of selected

The audit committee Chair plays an important role in leading and guiding discussions at audit committee meetings. The Chair should be independent, and have the right interpersonal skills to guide discussions on complex and sensitive matters.

(Appendix AAR: 8.1D)

board or council members, having at least 1 appropriately skilled audit committee member who is completely independent of the board or council can bring fresh insight or bridge gaps in the experience needed by the audit committee to perform their duties.

While the Director General or CEO should not be a member of the audit committee, it is important that they can attend meetings as an observer to provide context on important issues impacting the entity where useful or necessary, preferably meeting with the committee at least annually.

Collective expertise that is relevant to the entity

The audit committee must collectively have the knowledge, skills, qualifications and experience to perform its functions. As a minimum, the committee should comprise members with financial, risk management and relevant public sector or industry experience. Having a broad range of members from differing backgrounds helps to bring diverse perspectives to important issues and minimises group-think. Members should have senior governance and leadership experience in operating environments similar in complexity to that of the entity the audit committee is overseeing. Familiarity with the public sector environment of heightened probity, transparency and accountability is essential. If a new member does not have demonstrated experience working in or with the public sector, they must at all times fully inform themselves of their obligations and those of the entity. In these circumstances, induction and ongoing mentoring by the CAE, Chair and other members is important to support their contribution to committee effectiveness.

The skills and capabilities needed can vary over time, and will vary depending on the nature of the entity's activities. For example, if the entity is undergoing significant changes to information systems, the accountable authority may wish to consider appointing a member with IT operations or project leadership experience. Alternatively, audit committees can also use specialists or experts to help in the discussion of complex matters.

Leadership and interpersonal skills

Members, and in particular the Chair, need the right leadership and interpersonal skills to make committee meetings effective. Members need to feel confident to respectfully and, where necessary, persistently probe management, and to make useful contributions throughout the meeting. Much has been written on the qualities that make an effective committee member and these are relevant to public sector audit committees, recognising that public sector audit committees do not have decision-making authority or formal governance responsibility.

The committee needs at least three members

There is no specific number of members for a strong effective audit committee. However, audit committees should have at least 3 members². In determining the appropriate number of members, the accountable authority should consider what skills and experience is required based on the nature of the entity and its operations. Too few members may mean the committee does not have the extent of experience and knowledge to make informed decisions, and too many members may hinder robust discussion and debate.

Large complex State entities may choose to consider whether it is appropriate to establish the role of special advisers to the audit committee, within their charter. Senior managers appointed as special advisers participate like other audit committee members, but do not have formal membership status or 'voting' rights. They are there to provide operational context and detail to the committee. This is particularly important for audit committees

² For State entities refer to Treasurer's instruction 1201: 'Internal Audit' guidelines. For local government entities refer to section 7.1A of the *Local Government Act 1995*.

comprising mainly external members. These senior executives gain a valuable professional development opportunity from working closely with the committee, who are often senior governance professionals, and the opportunity to view their organisation from an oversight perspective.

2.3 Enabling robust discussions at audit committee meetings

Robust and respectful discussions between the audit committee, management and auditors are essential to good audit committee outcomes. It is important that the secretariat and CAE spend sufficient time planning audit committee meetings to facilitate these important discussions and achieve required outcomes.

Merely providing data/information versus delivering clear messages

Overwhelming the committee with data or information is unlikely to result in effective meetings and discussions. Information must be meaningful and fit for purpose. The CAE role in the audit committee meeting is more than simply gathering and transmitting information between management and the audit committee. The CAE should apply their professional expertise to deliver clear messages for audit committee deliberations. This is particularly important when the internal audit function is outsourced, as the CAE needs to ensure that the information meets the needs of the entity. Summary papers, which succinctly explain the issue and actions for the audit committee, are a good way to achieve this.

Having the courage to challenge

A good indicator of an effective audit committee is whether management feel that they have been appropriately challenged during audit committee discussions. This requires courage from members to question and probe management when necessary. Members should not take management assertions at face value, they should ask probing questions to ensure that the issue is not more significant than they are led to believe, or to make sure that a management action has actually been performed.

When management attend audit committee meetings, they should be prepared to answer challenging and difficult questions from audit committee members.

“Show me, don’t tell me”

Audit committees will need a level of evidence for assertions made by management, particularly around implementation of audit and review recommendations. They should be prepared to request from management all documentary information that the committee reasonably requires to satisfy themselves that key risks have been appropriately managed. The rigour and openness around evidencing management actions provides the audit committee insight into organisational culture and the commitment to accountability and transparency.

Having open discussions

Due to the advisory nature of the audit committee, they need capacity to discuss other matters which may not be included in the formal agenda. The agenda should allow for open discussion on other matters, as well as closed sessions with the CAE, internal audit teams or Office of the Auditor General (OAG). This will provide an opportunity for members to consider other matters which they would like to discuss and clarify.

2.4 Being aware of all assurance activities

It is vital that the audit committee has a sound understanding of the entity's assurance activities overall, as this provides valuable insights and direction to internal audit for its work program.

Assurance mapping can help to identify all assurance activities to ensure that the proposed internal audit plan focuses on areas where assurance is most needed.

When developing an internal audit plan, the committee should consider the following question:

'Is internal audit providing assurance on high risk activities, and considering where there are gaps in assurance?'

Using the fourth line of defence

Entities that use the fourth line of defence (external assurance) will be in a better position to coordinate their assurance activities. Having a complete picture of other assurance activities performed by the OAG, regulators or oversight committees, can help to identify gaps in assurance or potential risk exposures.

The audit committee should be aware of all external assurance activities, including OAG performance and focus audits and reports by other regulators or committees. Some examples of good practice behaviours we have observed at audit committees include:

- tracking and following-up the implementation of findings from OAG performance audits conducted within the entity
- performing self-assessments using the better practice information included in OAG focus and performance audits, and reporting the results back to the audit committee
- including the OAG audit committee briefing paper as part of meeting papers. This paper provides a regular snapshot of recently completed audits and audits in progress
- having a standing agenda item on fraud which provides a summary of relevant points from recently tabled Corruption and Crime Commission, Public Sector Commission or Parliamentary reports, or recent media coverage on fraud.

Understanding important financial reporting matters

Audit committees have an important role in overseeing financial and performance reporting within the entity. To perform this role effectively, it is critical that the audit committee has at least one member with a sound level of organisational-scale financial literacy.

Audit committee responsibilities for financial and performance reporting include reviewing financial statements and key performance indicators (State government entities) and recommending them for signature by the accountable authority, engaging with the OAG auditors during the financial audit, and reviewing and overseeing key controls related to financial reporting. It is a good idea to incorporate these reviews into the audit committee's annual work plan.

Best practice audit committees typically receive briefings on important matters or issues impacting risks, controls, financial and non-financial reporting. Figure 5 provides an example of how to report important control matters to the audit committee.

In order to review and endorse financial statements, audit committees need complete and accurate information about changes in accounting standards, accounting policies, judgements, estimates and errors.

Reporting a significant control matter to the audit committee

If an entity became aware that there was a significant payroll error or inappropriate use of a purchasing card, even if the amount in question was immaterial in value for the financial statements, such a matter would always be considered material in nature due to it representing a significant control breakdown or fraudulent activity.

In addition to reporting the matter to the Director General or CEO, the chief finance officer (CFO) would discuss the matter with the CAE and initially advise the Chair of the audit committee of the error and the actions taken or proposed to resolve it. The CFO should also raise the matter with the OAG financial audit team.

For the next audit committee meeting, the CFO and CAE should prepare a briefing for the committee on the matter, the likely impact and the actions taken or needed to correct the issue. The audit committee would consider the impact of the matter on risk assessments, external reporting and planned assurance activities. The committee would invite the CFO and representatives from human resources to the meeting to discuss the matter and obtain confidence around actions and improvements.

The committee would follow up to make sure control weaknesses were appropriately addressed and outcomes of any relevant investigations, disciplinary processes or referrals to integrity agencies.

Source: OAG

Figure 5: Advising the audit committee of significant control matters

Sharing information between the lines of defence

Management, in both the first and second lines of defence, frequently organise reviews and audits to assess maturity of their environment and identify business improvement opportunities. It is important that these activities are captured and shared with the CAE to help inform assurance mapping and allow for consolidated reporting of assurance activities to the audit committee. Visibility by the audit committee on management-initiated reviews helps to understand areas of risk management concern for management, systemic issues requiring improvement, and allows monitoring to ensure that internal auditors are not being used excessively by management and thus impairing their independence.

A central register for management reviews is useful to provide timely and collective information of past and current activities to improve controls and business performance.

2.5 Seeking assurance on organisational culture

Even though the culture of an entity cannot be seen, it is a fundamental part of strong governance (Figure 6).

Forward thinking accountable authorities and audit committees strive to maintain a sound culture within the entity to protect it from breakdowns in controls or fraud.



Source: OAG

Figure 6: Factors that contribute to a healthy organisational culture

Internal audit is in a good position to assess culture

Despite culture being a complex area to audit, internal audit is in a good position to provide assurance to the audit committee on it.

Culture auditing involves evaluating factors that influence behaviour and attitudes (soft controls) and examining hard evidence such as policies and employee surveys. Internal audit can assess culture in many ways. They can perform a specific audit covering culture, embed consideration in all potential internal audits, provide a general observation on culture in all audit reports or use it in root cause analysis for audit findings.

To embed culture into assurance practices, the 3 governance parties should:³

- give internal audit a clear mandate to audit entity culture and include the requirement in the internal audit charter
- set the right tone and demonstrate expected behaviours among others by practicing, measuring and assessing the culture of compliance with policies, procedures and controls
- understand the entity's culture risks including signs of negative leadership styles (autocratic, narcissistic, secretive, hypocritical, deflecting)
- observe culture indicators while performing internal audits
- have candid discussions on culture matters, e.g. being comfortable to talk about 'gut feel' and subjective judgements
- use a mapping tool to understand and assess the entity's culture and identify improvement opportunities. An example of such a tool is The Cultural Web⁴.

Do you know your culture indicators?
They include:

- trust
- openness
- honesty
- values
- behaviours
- leadership
- ethics.

Reporting culture to audit committees

Reporting to the audit committee about culture can be daunting for CAEs. Auditors typically like using hard, objective evidence to support findings. However, auditing organisational

³ *Organisational Culture: Evolving Approaches to Embedding and Assurance*, the Chartered Institute of Internal Auditors UK.

⁴ *The Cultural Web* is a tool used to map the culture of organisation, developed by Gerry Johnson and Kevan Scholes.

(Appendix AAR: 8.1D)

culture involves looking at soft indicators based on subjective judgements. To assist with this, internal audit can use metrics to support culture reporting. These are included in Figure 7⁵.

Objective metrics

Employee survey results, complaints, frequency and nature of legal issues, turnover statistics, frequency of repeat audit findings, frequency of large projects failing, timeliness and effectiveness of corrective actions, whistleblowing reports, loss events, compensation claims.

Subjective metrics

Lack of open communication (caused by fear, lack of trust, or information hoarding), excessive focus on short-term results, chronic grumbling by employees, gossip and rumours that lead to repercussions, 'my way or the highway' management approach that inhibits input and healthy debate, competition to get ahead rather than cooperation, lack of accountability from senior management.

Source: Institute of Internal Auditors Australia

Figure 7: Metrics for auditing culture

Audit committees and internal auditors should feel comfortable discussing aspects of culture. These include receptiveness by managers to scrutiny, the extent to which line areas view audit as a continuous improvement opportunity and management's general understanding of accountability and probity obligations in the public sector. Discussions of this nature may be more constructive during the routine closed-door sessions between independent committee members and auditors, without management present.

⁵ The Institute Internal Auditors *Auditing Culture: Observation and Data*, article by James Roth.

Part 3: Principles for better practice audit committees

The following section outlines better practice principles for public sector entity audit committees. These principles are based on the IIA's six key elements of effective audit committees which they use in their maturity model. The requirements for State and local government entities can be different, and entities should adapt these principles accordingly.

1. Membership: Members have the right experience and leadership skills to be trusted independent advisors.	
<p>1.1 Members are independent:</p> <ul style="list-style-type: none">• The audit committee has an independent external Chair.• Members are independent from the day-to-day management of the entity. This may not always be possible, but we recommend that the majority of members are independent of management.• The Director General, CFO or CEO are not members of the audit committee. However, they may attend meetings as observers or advisors. <p>1.2 The Committee has the right number of members:</p> <ul style="list-style-type: none">• The committee consists of at least 3 members.• For entities with boards/councils, the audit committee acts as a sub-committee and is not the entire board/council. We recommend a maximum of 5 members. <p>1.3 Members have the right skills and experience:</p> <ul style="list-style-type: none">• All audit committee members and the CAE are formally appointed by the accountable authority.• As a collective group, members have the right skills, experience and knowledge to competently perform their duties. At a minimum, the committee should comprise of members with financial, risk management and relevant industry or public sector experience.• The independent Chair should have the right interpersonal and leadership skills to effectively run the committee. An understanding of financial and other reporting requirements is also important. For State entities, the Chair should have membership in a professional accounting body or the IIA, or appropriate financial experience.	<p>1.4 Membership terms are appropriate:</p> <ul style="list-style-type: none">• Members are appointed for a minimum term of at least 3 years. To ensure that the committee has fresh insight and perspective, we would not recommend exceeding a term of around 6 years.• The accountable authority can terminate committee members for poor performance.• Appointments are staggered where possible to ensure continuity and clear succession for the audit committee Chair. <p>1.5 Members receive a formal induction:</p> <ul style="list-style-type: none">• The entity has a formal induction process for members that includes an information briefing, site visits (where relevant) and discussions with the CAE and accountable authority, including around the applicable legislative framework, probity, transparency and accountability obligations and expectations.• The Chair meets with new members to provide an overview of the committee and outline member expectations. <p>1.6 The committee has access to external auditors:</p> <ul style="list-style-type: none">• The committee requests an external auditor to attend meetings as an observer. <p>1.7 The Committee can seek advice when needed:</p> <ul style="list-style-type: none">• The audit committee charter allows the committee to obtain expert advice when needed.• The committee uses existing expertise within the entity to provide briefings on emerging risks, issues or matters which can help improve the member's understanding of the entity.

2. Roles and responsibilities: The roles and responsibilities of the audit committee allow for wholesome oversight of internal audit, governance, risk management and internal control practices.

2.1 Roles and responsibilities are clearly documented in the audit committee charter:

- The audit committee charter clearly defines the independence, accountability, role and responsibilities and reporting arrangements for the committee.
- The roles and responsibilities of the committee are consistent with legislated power and duties.
- The internal audit charter aligns with the audit committee charter.

2.2 Audit committee roles and responsibilities allow for comprehensive oversight:

- The charter clearly outlines the committee's responsibility for overseeing governance, risk management, internal controls and compliance.
- The audit committee functions include overseeing activities that help entities achieve their strategic objectives.
- The charter allows the audit committee to consider innovation and improvement ideas.
- The committee's charter allows it to monitor emerging risks and business practices.
- Where controls are managed by another entity under a shared service arrangement, the audit committee has a process to obtain comfort from the service provider that the controls are operating effectively. For example, the service level agreement or memorandum of understanding for the arrangement allows the entity's audit committee to request appropriate assurance from the service provider.
- Arrangements for shared audit committees or internal audit functions are clearly documented in the audit committee charter (if applicable).

2.3 The audit committee charter is appropriately approved and regularly updated:

- The audit committee and accountable authority formally approve the audit committee charter.
- The audit committee review and update the audit committee charter annually.

- The CAE monitors changes in practice (e.g. changes in the Institute of Internal Auditors' Professional Practice Framework (IPPF)) or other legislative or regulatory changes and suggest amendments to the committee as appropriate.

2.4 Audit committee members seek to continuously improve their skills and understanding:

- The CAE provides the committee with regular information on trends and emerging issues relating to governance, risk and compliance.
- Audit committee members endeavour to maintain current and relevant knowledge by seeking additional information where required. For example, requesting information from management about a particular function performed by an entity or by attending staff training on governance matters.

2.5 Members are aware of legislative and regulatory requirements, standards and guidance:

- Members are aware of all regulatory requirements, standards and guidance relevant to the entity. Four important requirements include:
 - State Financial Framework - Financial Administration Bookcase, including Treasurer's instruction 1201: 'Internal Audit' for State government entities
 - *Local Government Act 1995* and associated regulations
 - Requirements of effective internal audit functions as prescribed by the IPPF
 - Entity-specific legislation and regulatory compliance obligations. This can be found in the entity's annual report.

2.6 The committee does not make management decisions:

- The Audit Committee does not, and cannot, get involved in the day-to-day decision making by the entity. The committee can provide advice on important matters, but the responsibility for approving decisions must rest with the accountable authority or the CEO.

(Appendix AAR: 8.1D)

3. Professional practices: The audit committee conducts itself professionally to provide independent, sound and valuable advice to the accountable authority.

3.1 Conflicts of interest are considered and managed:

- Potential new members are required to declare any actual or perceived conflicts of interest.
- Processes for declaring and managing conflicts of interest are included in the audit committee charter and the service agreement (where relevant) for audit committee members.
- Members declare any conflicts of interest at the start of each meeting.

3.2 Meetings are regularly scheduled and include private sessions with important stakeholders:

- The audit committee meets at least four times a year, with capacity to meet at other times when necessary to perform a function (such as reviewing the financial statements and key performance indicators).
- The CAE regularly meets with the audit committee privately to discuss issues, management attitudes and risks.
- During the financial audit exit meeting with the OAG, the audit committee has a closed-door session with the auditors without management present. This provides a frank and open opportunity for the auditors to discuss how the audit went, whether they received the information they needed and whether there are any concerns with management behaviour that the committee should be aware of.
- The audit committee schedules private meetings with the accountable authority from time to time.

3.3 Key activities are scheduled in a forward work plan:

- Key activities of the audit committee are planned and scheduled in a forward work plan.
- CAEs monitor the forward work plan to determine what information and support the audit committee might need.

3.4 Members attend all meetings where possible:

- Meetings are scheduled in advance to facilitate 100% attendance of audit committee members.

3.5 Members share responsibility and act independently:

- Audit committee members function as a collective advisory group and share responsibilities equally.
- All members maintain their independent stance at all times, even if they are not independent of management.

4. Performance and accountability: The audit committee is aligned with the entity's strategic outcomes and is accountable for its performance.

4.1 The audit committee has mechanisms to assess its performance:

- The charter outlines expectations of the audit committee and includes processes to monitor and measure performance. These can include an annual self-assessment and regular independent reviews of the audit committee.

4.2 Meeting minutes are prepared and distributed to members quickly:

- Meeting minutes are distributed to members within the agreed timeline in the audit committee charter. A 2-week timeframe is commonly used in practice.

4.3 Attendance is monitored:

- The CAE or secretariat monitors attendance by audit committee members and implements alternative measures (e.g. virtual meetings) where necessary.
- The charter clearly outlines the minimum number of members for a quorum. The CAE or secretariat actively monitor whether there will be a quorum and reschedule the meeting if necessary.

4.4 Action items are followed-up and addressed promptly:

- Any action items arising from audit committee meetings are recorded and promptly distributed to the responsible officer for actioning.
- The implementation of action items is monitored and evidenced.
- The audit committee papers include a standing agenda item on the status of action items. There should be enough information in the papers to allow the audit committee to understand the nature of actions taken to date and the real reasons for any delays.

4.5 The committee has unrestricted access to the governing body and senior management:

- The audit committee charter allows the audit committee to access the Board, Council, CEO and senior management where necessary to discuss important matters.

4.6 Annual self-assessment by members:

- The audit committee performs an annual self-assessment to ensure it is operating effectively.
- The committee seeks feedback from observers from time-to-time to inform this assessment.

4.7 Periodic, independent assessment of committee performance:

- There is an independent assessment of the audit committee periodically (e.g. every 3 to 5 years) in conjunction with the independent assessment of the internal audit function.

4.8 The committee models the values and desired culture of the entity:

- The audit committee demonstrates the right tone and culture for the entity. For example, holding management to account for delays in implementing actions is one way to set a good tone within the entity.
- Committee members adhere to the entity's code of conduct. For example, members keep information confidential and conduct themselves in a professional and respectful manner.

4.9 Activities are aligned to the strategic mission of the entity:

- The committee understands the entity's strategic plan and direction and reflects on this when discussing the internal audit plan or risks.

(Appendix AAR: 8.1D)

5. Entity relationships: The audit committee is a trusted, independent partner.

5.1 There are regular meetings to build and maintain effective relationships:

- The audit committee Chair regularly meets with the accountable authority.
- The accountable authority sees the audit committee as a strategic partner and communicates with the Chair openly.
- The accountable authority shares important information about issues or risks openly with the audit committee, and meets with the committee at least annually.

5.2 The committee obtains information from executive management:

- The audit committee receives regular briefings from executive management on key matters related to their operations. For example, information on significant projects, long outstanding audit recommendations or emerging risks.
- Senior management use the collective experience and wisdom of the audit committee to guide their actions on important matters.

5.3 The committee uses expert advice where necessary:

- The audit committee accesses external expert advice when needed to support their deliberations. For example, the audit committee may wish to obtain independent legal advice to help them understand a significant issue raised in an internal audit report.

5.4 Entity staff are aware of the audit committee and internal audit:

- Information on the audit committee's role, functions and responsibilities, as well as the services offered by internal audit, is available on the entity's intranet.
- The induction process for senior executives includes a meeting with the CAE and the Chair of the audit committee.

6. Governance and reporting: The audit committee is governed effectively to enable transparent, objective and timely reporting.

6.1 There are dedicated secretariat resources:

- The committee has sufficient secretariat support to plan and document meetings.
- The CAE oversees the secretariat in preparing agendas, meeting papers and reviewing minutes and discusses these with the Chair for approval.

6.2 The committee maintains independence safeguards:

- The audit committee always acts to protect the independence of the internal audit function and the CAE.

6.3 Conflict of interest procedures are adhered to:

- Members declare all actual, perceived and potential conflicts of interest at the start of each meeting.
- Other conflict of interest processes, such as annual declarations, are adhered to and monitored by the audit committee and CAE.

6.4 Audit recommendations are recorded and monitored:

- A log of outstanding audit recommendations is prepared for each audit committee meeting. This log should include the recommendations from all internal, financial and performance audits conducted within the entity.
- Agreed actions to address the recommendations are clearly articulated and reported accurately to the audit committee in the log.
- Internal audit has a framework to review and close-out audit recommendations that suits the entity's needs. This framework should be approved by the audit committee.
- Audit committee members monitor the implementation of recommendations and challenge management to ensure that actions are actually implemented.

6.5 The accountable authority is adequately briefed:

- The audit committee, with the assistance of the CAE, provides a briefing to the accountable authority after each meeting on key issues or risks.

6.6 The Audit committee regularly reports on its performance:

- The entity's annual report includes information about the audit committee and outcomes delivered during the period.

Part 4: Guidance for audit committee fees

The appointment of independent audit committee members, who are external to the entity, will raise consideration of whether they are entitled to be reimbursed for their services.

There is some guidance in the *Premier's Circular 2019/07 - State Government Boards and Committees* regarding the payment of fees to committee members. Generally, fees cannot be paid to people who are full time State, Commonwealth and local government employees, Members of Parliament, current and retired judicial officers (except Magistrates) and current non-academic employees of public academic institutions. Entities should be aware of the requirements of this circular, and other legislation and regulations, when determining whether a fee can be paid to an external member.

Guidance for determining fees

Any fees paid to external audit committee members should reflect their role on the committee and associated responsibilities and expertise. For example, the audit committee Chair may need a different level of remuneration to other external members as they perform additional duties, such as having regular discussions with key governance parties, including the CAE and accountable authority.

Some items which entities may wish to reimburse members for include:

- meeting attendance and preparation time (this could be a fixed amount per meeting or an hourly rate)
- travelling expenses
- accommodation expenses.

When determining fees paid to external members, the entity and the member need to clearly agree on the hourly rates, generally with an upper limit of the amount of hours required to perform their duties, or a fixed annual fee, and the extent of reimbursements allowed. Entities should clearly document these arrangements in a services agreement. TI 1201 includes a template services agreement for engaging an independent external Chair. The template includes set terms and conditions relating to payment of fees. While this is not compulsory, entities should consider using it to help develop service agreements.

State entities can use the Common Use Agreement on Audit and Financial Advisory Services as a guide or benchmark for remuneration.

Entities should ensure that they comply with relevant procurement policies or requirements when obtaining external members.

Part 5: Guidance for smaller entities

We recognise that it is difficult for smaller entities, particularly those located in regional or remote locations, to establish audit committees that meet all of the better practice principles outlined in this guide. However, the risks to good governance remain very real in these entities too. This section provides guidance for smaller entities to help them improve the effectiveness of their audit committee.

Financial risk expertise is essential

While the functions of the audit committee are diverse, overseeing financial and performance reporting processes, and their associated internal controls, are incredibly important. Audit committees can help to prevent fraud by:

- understanding and challenging management about the accounting treatments, judgements and estimates used to prepare financial statements
- engaging with the OAG and management about deficiencies in internal controls and the actions needed to remediate these.

To do this effectively, at least one audit committee member needs to have an understanding of financial reporting and accounting standards, and the role of internal and external audit.

When trying to find members with financial reporting experience, smaller entities may wish to consider sharing resources with similarly sized entities. For example, a local government entity could consider the suitability of an accountant from a neighbouring shire as an independent audit committee member, or a suitably experienced person from a larger local government entity could be an audit committee member if they can perform their role remotely.

Smaller size does not mean smaller risk

Smaller entities are often exposed to unique inherent risks such as limited segregation of duties and potential conflicts of interest issues associated with a limited number of suppliers in regional areas. Not managing these risks properly can increase the risk of fraud or error.

The meeting agenda and annual work plan templates, provide additional guidance on the matters which should be considered in audit committee meetings. These templates are included in the toolkit.

Audit committees need to be aware of these risks and ensure that there is independent oversight of the processes to manage them. For example, regular internal audits on procurement which look at the processes for managing conflicts of interest can help provide assurance to the committee. In addition, risk management training for audit committee members can help them understand and assess risks relevant to smaller entities.

Sharing resources may help bridge gaps

Smaller entities, who deliver similar services to the community, may benefit from sharing resources to help build the capability of their internal audit function and audit committee. This could be achieved by using a shared internal audit service. State government entities have the option to consider sharing their audit committee with another entity, provided that committee members have a sound understanding of both entities' operations, culture and goals and devote adequate time to oversee each entity.

Roles and responsibilities must be clearly communicated during induction

The audit committee may include members with varied experience that bring valuable insights to entities. However, there is a chance that members may not have any previous

audit committee experience. This means that having an effective induction process, which clearly explains roles, responsibilities and expectations is vital. Smaller entities may wish to consider additional training or guidance to help them understand their important role.

To assist smaller entities with their induction processes, we have included an induction checklist in the Toolkit.

Getting the most from the fourth line of defence

Smaller entities should use information and guidance from external sources, such as the OAG, parliamentary committees, Public Sector Commission and Corruption and Crime Commission as much as possible to assess their systems of risk management and internal controls. For example, information from OAG audit reports can help entities understand common risks in the sector, and frequently contain better practice guidance which smaller entities can self-assess against.

External auditors can provide valuable perspective

The OAG, and their contracted auditors are independent, and can provide information on whether controls are operating effectively. To facilitate good discussions between the OAG, management and the audit committee, it is essential that all parties discuss issues openly and frankly. For example, local government entities may wish to consider suspending standing orders at audit entrance and exit meetings to allow the audit committee, management and the auditors to have robust discussions.

Seeking independent assurance when one person performs many roles

Smaller entities may have one person (such as the CEO or executive manager of corporate services) responsible for multiple functions such as risk management, compliance and internal audit. This can create a self-review risk, if they are being asked to report on the effectiveness of all of these processes to the audit committee.

Audit committees need to be aware of these risks and put strategies in place to provide a level of independent assurance about these important functions.

Audit recommendations need prompt action

Smaller size entities have fewer staff and this may make it more difficult to resolve audit recommendations quickly. Given the inherent risks associated with smaller entities mentioned above, it is vital that the audit committee insists that control deficiencies, particularly those that could result in the misappropriation of assets, are prioritised and actioned and documented promptly.

Audit committees need good support

Timely and succinct reporting is important to demonstrate that the audit committee is accountable for its governance role. This means that it is important that minutes of meetings and any action items, or requests for further information are actioned and documented promptly.

Part 6: Toolkit

The toolkit contains a number of templates that public sector entities may find useful to help establish and maintain an effective audit committee. The templates help to promote the better practice principles included in the guide and are designed to be easily tailored to meet the entity's specific circumstances.

Entities should take care to modify the tools to reflect their legal or regulatory requirements. For example, local government entities will need to adapt these templates to address the specific requirements of the *Local Government Act 1995* and relevant regulations.

These tools may be updated from time to time. Please check our website for the latest version.

List of tools

- 1 Example audit committee charter
- 2 Audit committee member induction checklist
- 3 Meeting preparation checklist
- 4 Meeting agenda template
- 5 Characteristics of effective meetings
- 6 Annual work plan template
- 7 Audit recommendations progress report template
- 8 Review of the OAG audit reports template

Tool 1 Example audit committee charter

The following example is designed to assist accountable authorities and audit committees develop an audit committee charter that reflects our better practice principles.

Source: OAG using information from the Institute of Internal Auditors Australia and Australian National Audit Office

ENTITY NAME

AUDIT [AND RISK ASSURANCE⁶] COMMITTEE CHARTER

Role

The accountable authority has established the audit committee under [Insert the related legislative/regulatory reference].

The audit committee assists the accountable authority in fulfilling their oversight responsibilities in relation to systems of risk management and internal control, the entity's processes for monitoring compliance with laws and regulations, including the code of conduct, financial and performance reporting and external and internal audit. The audit committee is not responsible for the management of these functions.

The audit committee will engage with management in a constructive and professional manner to perform its oversight responsibilities. The Chair of the audit committee is responsible to, and reports to the accountable authority.

Members of the audit committee are expected to:

- understand the legal and regulatory obligations of the accountable authority for governing the entity
- understand the department's/statutory authority's/council's governance arrangements that support achievement of the department's/statutory authority's/council's strategies and objectives
- exercise due care, diligence and skill when performing their duties
- adhere to the entities code of conduct and the code of ethics of any professional body which they are a member of
- help to set the right tone in the entity by demonstrating behaviours which reflect the entity's desired culture
- be aware of contemporary and relevant issues impacting the public sector
- only use information provided to the audit committee to carry out their responsibilities, unless expressly agreed by the accountable authority.

To help support the audit committee's role in overseeing the internal audit function, the Chief Audit Executive will functionally report to the audit committee.

The audit committee will prepare an annual work plan that outlines when it will perform key activities, in consultation with the accountable authority.

⁶ Most public sector entities do not have a separate sub-committee for overseeing risk management in the entity. It is therefore common for the audit committee to take on this role.

(Appendix AAR: 8.1D)

Authority

The accountable authority authorises the audit committee, in accordance with this Charter, to:

- obtain any information it requires from any official or external party (subject to any legal obligation to protect information)
- discuss any matters with the internal auditors, Office of the Auditor General (OAG), or other external parties (subject to confidentiality considerations)
- request the attendance of any official, including the accountable authority, at audit committee meetings
- obtain legal or other professional advice when necessary to fulfil its role, at the entity's expense, subject to approval by the accountable authority or delegate
- provide advice to the accountable authority on the appointment and replacement of the chief audit executive of the [department/statutory authority/council](#).

The audit committee may undertake other activities as requested by the accountable authority.

Membership

The audit committee comprises [\[insert number/up to\]](#) members of whom [\[insert number/at least\]](#) must be independent, appointed by the accountable authority. The committee will be led by an independent Chair, appointed by the accountable authority. The Chair will be appointed for an initial period of [\[insert number of years\]](#) and may be extended or reappointed for further periods as determined by the accountable authority.

Audit committee members will be appointed for an initial period of [\[insert number of years\]](#) as determined by the accountable authority.

The accountable authority will review the membership of the committee every [\[insert number of years\]](#) to ensure that there is an appropriate balance between continuity of membership, the contribution of fresh perspectives and a suitable mix of qualifications, knowledge, skills and experience. The accountable authority may choose to re-appoint members based on their ability to contribute to the work of the audit committee. However, the total length of time a member can sit on the committee will not exceed [\[insert number of years\]](#).

The accountable authority may remove an audit committee member at any time before their term expires, or a member may resign.

Audit committee members will collectively have a broad range of skills and experience relevant to the operations of the [department/statutory authority/council](#). At least one member of the audit committee will have accounting or related financial management experience, with an understanding of accounting and auditing requirements in the public sector. To support the skills and experience of committee members, the committee will implement an induction and training program for new members.

The audit committee may invite the accountable authority, chief executive officer, chief financial officer, chief information officer, chief audit executive, or other management representatives to present information and participate in the meeting. An officer from the OAG will be invited to attend audit committee meetings as an observer.

The audit committee will be administratively supported by a secretary who is appointed by management.

Responsibilities

The audit committee will be responsible for the following:

The following part of the model charter provides an extensive list of many functions that the audit committee can perform. It is not intended that entities copy all of the functions in these lists. Instead, the accountable authority should review and modify the functions to suit the entity. It is important that the accountability authority and the audit committee agree on these functions.

Risk management, fraud and internal control

The audit committee oversees the entity's system of risk management and internal controls. Its responsibilities include, but are not limited to:

- providing oversight on significant risk exposures and control issues, including fraud risks, governance issues and other matters as necessary or requested by senior management and the accountable authority
- considering the impact of [department's/statutory authority's/council's](#) culture on risk management and internal controls
- annually reviewing the [department's/statutory authority's/council's](#) assurance map to ensure that risk and control activities are coordinated, communicated and managed effectively
- annually reviewing the [department's/statutory authority's/council's](#) risk management framework
- monitoring changes in government strategies, the economic and business environment and other trends and factors related to the [department/statutory authority/council's](#) risk profile. This includes meeting periodically with key management, internal auditors, the OAG, and compliance staff, to understand and discuss the impact of these changes or trends on the risk profile
- reviewing whether the [department/statutory authority/council](#) has an effective risk management framework, and, based on knowledge and understanding of the entity's risks, that material business risks are appropriately reflected in the risk profile and reported to the accountable authority
- reviewing and assessing the effectiveness of processes for identifying, managing, treating and mitigating the [department/statutory authority/council's](#) risks and ensuring that remaining risks align with the entity's risk appetite. The committee should prioritise risks involving:
 - significant business risks, including environmental and occupational health and safety risks
 - potential non-compliance with laws, regulations and standards
 - fraud and theft
 - litigation and claims.
- considering the adequacy and effectiveness of internal controls and the risk management framework by:
 - reviewing reports from management, internal audit, consultants, regulators and the OAG

(Appendix AAR: 8.1D)

- ensuring risk registers consider risks that may impact whether the entity will achieve its strategic objectives
- reviewing management's response to IT risks, including cyber risks
- monitoring management responses and ensuring timely correction actions are taken by management
- understanding the process of managing insurable risks and assessing whether the [department/statutory authority/council](#) has adequate insurance cover for these risks
- assessing the effectiveness of, and compliance with, the entity's code of conduct
- assessing whether management has controls in place for non-routine types of transactions and/or any potential transactions that might carry an unacceptable degree of risk
- enquiring with management and the OAG regarding their assessment of the risk of material misstatement in the financial report due to fraud
- enquiring with management, internal auditors and the OAG about whether they are aware of any actual, suspected or alleged fraud or corruption affecting the [department/statutory authority/council](#) including the entity's response to the matters
- reviewing the [department/statutory authority/council's](#) processes and systems to detect, capture and respond to fraud risks, including preventative measures
- reviewing the business continuity planning process and be assured that material risks are identified and appropriate business continuity plans, including disaster recovery plans, are in place.
- reviewing summary reports from management on all suspected, alleged and actual frauds, thefts and breaches of laws and ensuring these are reported to the accountable authority and/or relevant authorities
- reviewing summary reports from management on communication from external parties including regulators that indicate problems in the internal control system or inappropriate management actions
- liaising with other subcommittees on matters relating to risk management, fraud and internal control
- [\[for entities who use a shared service arrangement\]](#) reviewing comfort letters and other assurance reports regarding the effectiveness of controls managed by shared service providers on behalf of the entity.

Internal audit

The audit committee is responsible for guiding and overseeing the activities, resources and structure of the internal audit function. The audit committee's responsibilities include, but are not limited to:

- annually reviewing internal audit's mission, resources and budget and protecting internal audit's independence from management
- reviewing the internal audit structure, composition, skills and experience, service delivery model, independence and access to the [accountable authority/board of directors](#)

(Appendix AAR: 8.1D)

- advising the accountable authority on the appointment and replacement of the chief audit executive
- advising the accountable authority on the adequacy of internal audit resources or budget to perform the approved internal audit plan
- ensuring that the internal audit function, through the chief audit executive, has a direct reporting relationship with the audit committee and accountable authority (functional reporting relationship) and has access to all levels of management needed to perform their duties
- monitoring internal audit's participation in non-assurance roles to assess whether it impacts their independence or interferes with the delivery of the internal audit program
- assessing the internal audit plan to ensure that it comprehensively covers material business risks that may threaten the achievement of strategic objectives and allows internal audit to assess culture
- reviewing and recommending the approval of the internal audit plan and work program by the accountable authority
- communicating the audit committee's expectations to the chief audit executive in writing through the internal audit charter
- reviewing the internal audit charter annually for the accountable authority's approval
- reviewing the quality and timeliness of internal audit reports
- considering the implications of internal audit findings on the business, its risks and controls
- monitoring management's implementation of internal audit recommendations
- monitoring the progress of the internal audit plan and work program
- monitoring the quality of internal audit services delivered and compliance with the Institute of Internal Auditors' International Professional Practices Framework
- overseeing the coordination of planned activities between the 4 lines of defence
- reviewing the annual report from the chief audit executive or the internal audit service provider on the overall state of the [department/statutory authority/council's](#) internal controls
- ensuring that internal audit has complete and timely access to all accounts, information, documents and records of the entity as needed to effectively perform their duties. This also includes discussing whether management was cooperative and provided timely responses to internal audit requests
- meeting privately with the chief audit executive at least once per year.

Compliance and ethics

The audit committee oversees the [department/statutory authority/council's](#) processes to ensure compliance with relevant laws and regulations and for promoting a strong governance culture within the entity. This includes, but is not limited to:

- understanding the [department/statutory authority/council's](#) compliance framework including its obligations, the officers responsible for compliance activities and management oversight and review of these processes

(Appendix AAR: 8.1D)

- considering the impact of [department/statutory authority/council's](#) culture on compliance processes
- overseeing compliance by reviewing arrangements that monitor the impact of changes in key laws, regulations, internal policies and accounting standards affecting the [department/statutory authority/council's](#) operations
- reviewing management's investigation of non-compliance matters and obtaining assurance from management that appropriate follow-up action was taken
- obtaining updates from management on matters of compliance and ethical matters that may have material impact on the [department/statutory authority/council's](#) financial statements, strategy, operations, health and safety or reputation
- reviewing and monitoring related party transactions and conflicts of interest
- enquiring with management, internal audit and the OAG on their assessment of the compliance culture, the risk of non-compliance, or whether they have any knowledge of any actual, suspected or alleged non-compliance affecting the entity
- overseeing complaints management and whistleblowing policies to ensure that they are recorded and actioned effectively
- reviewing the [department's/statutory authority's/council's](#) processes for communicating, and assessing the effectiveness of, the entity's code of conduct
- meeting with management to discuss regulatory compliance matters the [department/statutory authority/council](#) has considered in the preparation of the financial statements, such as compliance with accounting standards.

Financial and performance reporting

The audit committee oversees the integrity of financial and performance reporting processes within the entity. The committee's responsibilities include:

- reviewing the financial statements and providing advice to the accountable authority about whether they should be signed by the accountable authority. The review includes assessing:
 - whether the financial statements are consistent with the knowledge of the audit committee members
 - whether the financial statements comply with [\[Insert the related legislative/regulatory reference\]](#)
 - whether the financial statements accurately reflects the entity's financial position and performance, and if not, whether additional disclosures are required
 - the appropriateness of accounting policies and disclosures, including changes to accounting policies
 - areas of significant judgement, estimation and significant or non-routine transactions
 - whether appropriate management action has been taken in response to any issues raised by the OAG, including financial statement adjustments or revised disclosures
 - the quality of the entity's processes for preparing the financial statements, including how management has checked that they comply with relevant requirements

(Appendix AAR: 8.1D)

- significant issues, errors or discrepancies in the draft financial statements and ensuring members understand the reasons why these occurred
- the representation letter to be provided to the OAG to confirm that the assertions, including any immaterial errors collated during the audit, are appropriate.
- acting as a forum for communication between management and the OAG
- reviewing the entity's process to ensure the financial information included in the annual report is consistent with the audited financial statements
- [For State government entities only] reviewing the entity's systems and procedures for assessing and reporting on the [department's/statutory authority's](#) performance through key performance indicators. This includes determining whether:
 - the key performance indicators are relevant and appropriate to assess the entity's performance and take into account guidance issued by the Department of Treasury
 - the [department/statutory authority](#) has sound processes and controls for measuring and reporting on key performance indicators in its annual report
 - the key performance indicators are consistent with the entity's financial information, including its financial statements, that it proposes to include in its annual report
 - there are reasonable disclosures to explain why there is a significant variation in performance.

External audit

The audit committee is responsible for communicating and liaising with the OAG. This includes understanding the results of financial and performance audits conducted within the entity and overseeing whether recommendations are implemented by management. The committee's responsibilities include, but are not limited to:

- meeting with the OAG to discuss the audit plan (audit entrance meeting) and the results of the financial audit (audit exit meeting)
- discussing with the OAG any significant resolved or unresolved disagreements with management
- monitoring and critiquing management's response to OAG findings and recommendations
- reviewing reports from the OAG including auditor's reports, closing reports and management letters
- reviewing all representation letters signed by management to assess whether the information appears complete and appropriate
- meeting with the OAG at least once per year without management presence. At this meeting, the committee will discuss matters relating to the conduct of the audit, including any difficulties encountered, restrictions on scope of activities or access to information, significant disagreements with management and adequacy of management responses
- reviewing performance audits conducted at the entity and ensuring that agreed recommendations are implemented
- monitoring the relationship between internal auditors and the OAG

(Appendix AAR: 8.1D)

- reviewing results of relevant OAG audit reports and better practice publications for guidance on good practices, including any self-assessment by management
- reviewing the form and content of the proposed auditor's report on the entity's financial and performance report. This may include any proposed modification, emphasis of matter, key audit matters, other matters and uncorrected misstatements in other information.

Other responsibilities

Perform other activities related to the role of this charter as requested by the accountable authority.

Administrative responsibilities

Meetings

The audit committee will meet at least 4 times a year or more frequently as necessary, depending on the size and complexity of the entity.

The Chair is required to call a meeting if asked to do so by the accountable authority. If a meeting is requested by another audit committee member, OAG or chief audit executive, the Chair will decide whether the meeting is necessary.

The Chair will oversee the planning and conduct of meetings including the approval of the agenda and draft minutes, and reporting to the accountable authority.

A quorum will consist of a majority of committee members. Where there is more than 1 external member on the audit committee, a quorum will include at least 1 external member. The quorum must be in place at all times during the meeting.

Secretariat

The accountable authority, in consultation with the audit committee, will formally appoint an officer to provide secretariat services to the committee. The secretariat will provide services as required by the audit committee that includes:

- preparing a meeting agenda for each meeting that is approved by the Chair
- circulating the meeting agenda and supporting papers at least 1 week before the meeting
- preparing minutes of the meetings and circulating them no later than 2 weeks after the meeting
- maintaining final meeting papers and minutes in accordance with the recordkeeping requirements of the [department/statutory authority/council](#).

Independence and conflicts of interest

The audit committee must be independent from management of the [department/statutory authority/council](#). Once a year, audit committee members will provide written declarations of any actual or perceived conflicts of interest to the accountable authority.

External members should consider past employment, consultancy arrangements and related party issues when making these declarations to the accountable authority. In consultation with the Chair, the accountable authority should be satisfied that there are sufficient processes in place to manage any actual, perceived or potential conflicts of interest.

(Appendix AAR: 8.1D)

At the start of each audit committee meeting, members are required to declare any personal interests that may apply to specific matters on the meeting agenda. The Chair, in consultation with the accountable authority where appropriate, is responsible for deciding if the members should excuse themselves from the meeting or from the audit committee's consideration of the relevant agenda item(s).

Details of any personal interests declared by the Chair and other audit committee members, and actions taken to manage the conflicts, should be appropriately recorded in the meeting minutes and the [department/statutory authority/council](#) register of conflicts of interest in accordance with its policy.

Audit committee performance assessment arrangements

The Chair of the audit committee, in consultation with the accountable authority, will review the performance of the audit committee annually, together with the annual review of this charter.

The review is performed using the approved assessment tool with appropriate input from the accountable authority, committee members, senior management, chief audit executive, and any other relevant stakeholders.

The Chair will provide advice to the accountable authority on the members' performance, particularly for external members, or members where an extension of tenure is being considered.

The Chair will always consider the costs and benefits of the activities that the audit committee performs.

Reporting

The audit committee will, as often as necessary, and at least once a year, report to the accountable authority on its operations and activities during the year and confirm to the accountable authority that all functions outlined in this charter have been satisfactorily addressed.

The audit committee may at any time, report to the accountable authority on any other matters it deems to be sufficiently important. In addition, any individual audit committee members may request a meeting with the accountable authority at any time.

Review of charter

The audit committee will ensure that this charter complies with relevant legislative and regulatory requirements and will propose amendments when necessary to ensure that it accurately reflects the committee's current role and responsibilities.

The audit committee will review this charter once a year and more frequently if required. The review will include consultation with the accountable authority. Any substantive changes to the charter will be recommended by the audit committee and formally approved by the accountable authority.

Endorsed:

Audit committee Chair

[Signature]

[Date]

Approved:

Accountable Authority

[Signature]

[Date]

Tool 2 Audit committee member induction checklist

This checklist includes a list of activities the Chief Audit Executive can use for inducting new audit committee members.

Source: OAG using information from the Institute of Internal Auditors Australia

Activity	Completed
Authority, composition and meetings	
Meet with all members of executive management.	
Read and understand the audit committee and internal audit charters.	
Read audit committee minutes for the last 3 years.	
External reporting	
Read and understand the entity's summary of significant accounting policies and significant judgements made in preparing the financial statements.	
Read and understand management's summary of processes for monitoring compliance with laws, regulations and other requirements.	
Read and understand the entity's processes for reporting to regulatory or oversight bodies (if any).	
Read and understand the entity's main corporate governance practices reported in its annual report for the last 3 years.	
Read the financial reports and any associated non-financial disclosures for the past 3 years.	
External audit	
Meet with the senior members of the OAG financial audit team.	
Read and understand the OAG's findings and recommendations, and management's response, for the last 3 years. This includes performance audits conducted at the entity.	
Internal audit	
Meet with the Chief Audit Executive (head of internal audit) and key audit team members (in-house, or outsourced firm partners and managers).	
Read and understand internal audit's mission, including its resources and budget structure.	
Read and understand the internal audit plan for the last 3 years.	
Understand the audit committee's expectations of the Chief Audit Executive.	
Read and understand all internal audit's findings and recommendations which remain unresolved.	

(Appendix AAR: 8.1D)

Activity	Completed
Read a sample of audit reports prepared by the internal audit area during the last 3 years.	
Read and understand the process the entity has in place for monitoring and assessing the effectiveness of the internal audit function.	
Read and understand the process for coordinating the planned activities of internal audit and the OAG, and risk and compliance management.	
System of internal control and risk management	
Meet with the Chief Risk Officer.	
Read and understand the risk management framework, assurance mapping and strategic plan.	
Meet with the Chief Information Officer to discuss information security processes and controls.	
Read and understand information related to the entity's identified tolerance for risk.	
Read and understand entity processes for identifying and managing material risks including business, financial, legal and compliance risks.	
Read summary reports from management on all suspected, alleged and actual frauds, thefts and material breaches of laws for the last 3 years.	
Compliance and ethics	
Read and understand the entity's processes for managing complaints and whistleblowing.	
Read significant issues, independent investigations and disciplinary action as reported to the accountable authority in the last 3 years.	
Attend a briefing or training on public sector probity and accountability requirements, including ethical considerations.	
Fraud	
Read and understand the entity's fraud prevention and detection framework and monitor suspected, alleged and actual instances of fraud.	
Read any instances of fraud reported during the last 3 years.	
Related-party transactions	
Read and understand processes for related-party transactions.	
Read related-party transaction reporting for the last 3 years.	
Governance framework	
Read and understand the governance framework and charter of the entity's other committees.	
Read and understand the organisational structure.	
Read and understand the entity's delegation schedule/register.	

Tool 3 Meeting preparation checklist

This checklist is to assist the secretariat in planning audit committee meetings. It's important to plan the date for each activity, working backwards from the meeting date, to ensure timely distribution of meeting papers to members and attendees.

Source: Australian National Audit Office

[Entity's name] Audit committee meeting

Meeting preparation checklist

Meeting Date: [insert date]

Audit Committee meeting	Planned Date	Completed Date
Members and observers' attendance confirmed.		
Room and required equipment booked (including 'members only' session).		
Chair and Chief Audit Executive discuss draft agenda based on committee work program and priority risks and issues		
Draft agenda circulated to Chair and members.		
Agenda confirmed with Chair		
Required papers collated. This includes, as appropriate:		
<ul style="list-style-type: none">list of attendees and apologies		
<ul style="list-style-type: none">minutes of previous meeting for review and confirmation		
<ul style="list-style-type: none">updated audit committee action item list with the status of actions arising from the previous meeting minutes		
<ul style="list-style-type: none">relevant information/papers from management		
<ul style="list-style-type: none">reports from internal audit		
<ul style="list-style-type: none">status report on implementation of previous internal and external audit, consultant and regulator report recommendations		
<ul style="list-style-type: none">reports from the OAG		
<ul style="list-style-type: none">compliance audit return (for local government entities)		
<ul style="list-style-type: none">report from the Chief Executive Officer under Regulation 17 of the Local Government (Audit) Regulations 1996 (local government entities)		
<ul style="list-style-type: none">reports prepared under section 7.12A of the <i>Local Government Act 1995</i> (local government entities)		
<ul style="list-style-type: none">other papers/information as reflected in the audit committee annual work plan.		
All papers marked with appropriate security classification.		

(Appendix AAR: 8.1D)

Audit Committee meeting	Planned Date	Completed Date
Agenda and papers distributed to members and attendees at least 7 days prior to meeting.		
Draft minutes prepared and circulated to members within 14 days of meeting.		
Revised minutes, reflecting changes made by committee members, sent out for final review.		

Tool 4 Meeting agenda template

This tool provides an example agenda for an audit committee meeting. The agenda should be based on the committee’s annual work program, with flexibility for additional emerging risks and issues.

Source: OAG

[Entity’s Letterhead]

[Entity’s name] Audit Committee Meeting

[Date and time]

[Venue]

Attendees

Name	Role / Position
Committee members:	
1. [List attendees and apologies – include name, state if Chair or secretary and if external or internal member]	
Observers	
2. [List attendees and apologies – include name and position]	
Apologies	
3. [List attendees and apologies – include name and position]	

Agenda	Owner (Insert name)	Action (Noting, Discussion, Approval)
1. Welcome and apologies		
2. Confirmation of minutes		
3. Declaration of conflicts of interest by audit committee members and observers		
4. Issues brought forward from previous meeting		
5. Action items from previous meeting		
6. Reports to be tabled (refer to annual work plan) <ul style="list-style-type: none">• Risk management• Internal control• Internal audit• Compliance• Financial reporting• Performance reporting• External audit		

(Appendix AAR: 8.1D)

Agenda	Owner (Insert name)	Action (Noting, Discussion, Approval)
• [name other items].		
7. Status of recommendations from internal audit, OAG and consultant or regulator reports		
8. Review of audit committee charter (annual item)		
9. Assessment of audit committee performance (annual item)		
10. Review of annual work plan (to identify issues and prepare for next meeting)		
11. Other business		
12. Next meeting		
13. Meeting close		

Tool 5 Characteristics of effective meetings

This tool contains guidance on how to conduct an effective meeting. Audit committees can use this guidance to assess how well the meeting was run.

Source: OAG

Characteristics of an effective meeting include a combination of the following:

Pre-meeting

- the audit committee Chair discusses key issues with the chief audit executive and approves the agenda before it is issued and members agree on key discussion points for each agenda item at the beginning of each meeting ('starring' of key items)
- meeting papers are presented in an agreed form and provided to audit committee members at least 1 week prior to the meeting. Meeting papers may need to be distributed to members earlier when there are complex matters to be discussed or approved
- each member is briefed before each meeting by the audit committee secretariat on major issues
- agenda items clearly indicate what action is required from the audit committee members, such as discussion, noting, endorsement, approval, presentation. This ensures that audit committee members know what is required at the meeting
- the Chair and Chief Audit Executive meet before each meeting to discuss the agenda and any priority issues they wish to discuss with management.

Meeting

- the audit committee meets privately before each meeting to discuss issues without management and other observers present
- meetings facilitate open and robust discussions
- all members are responsible for effective meetings and raising continuous improvement opportunities to the Chair, when identified
- meetings are not used to edit documents received by the committee for approval or endorsement. Minor edits should be provided to the Secretariat before or after the meeting
- at the start of each meeting, members declare any actual, potential or perceived conflicts of interest that they have with any agenda item
- any private meetings (i.e. with internal auditors or the OAG) should be held at the start or end of the meeting
- all audit committee members have read, and engaged with the meeting papers prior to the meeting
- important or contentious agenda items are first on the agenda to ensure that they are addressed in the meeting
- members reflect on what went well, or what needs improvement.

Tool 6 Annual work plan template

The following tool is an example of an annual work plan for audit committees to help schedule activities across the year. A minimum of four meetings per annum is recommended, often with a fifth focussed meeting for the financial statements.

Source: OAG using information from the Australian National Audit Office

[Entity Name] Audit Committee Annual Work Plan 202X- 202X⁷,

Functions, responsibilities and associated activities	Mar	Jun	Aug	Sept	Dec
1. Governance arrangements					
If required by the accountable authority, review the entity's governance arrangements or elements of the arrangements and suggest improvements where appropriate.		X			
Ensure that appropriate mechanisms are in place to review and implement relevant parliamentary committee reports, external reviews and evaluations of the entity, and recommendations arising from these reports and reviews.	X				
2. Risk management					
Review the risk management framework, risk register and fraud and corruption control plans to see that the risks represent and address the current environment and strategic direction of the entity, and meet legislative compliance and better practice principles.	X				
Consider the findings of the entity's occupational health and safety reviews and enquire of management the arrangements to address these.				X	
Consider emerging risks and current issues arising from major projects.	X	X		X	X
Determine whether the entity has a sound and effective approach for business continuity planning arrangements, including whether business continuity and disaster recovery plans have been periodically reviewed and tested.					X
Review reports on fraud that outline any identified allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risk.	X	X	X	X	X

⁷ The marking of 'X' is an example only.

(Appendix AAR: 8.1D)

Functions, responsibilities and associated activities	Mar	Jun	Aug	Sept	Dec
3. System of internal control					
Review management's approach to maintaining an effective system of internal control. This should include internal controls in relation to functions performed by external parties such as shared services providers, contractors and advisers.	X				
Obtain management assurances on the adequacy of internal controls and compliance by staff.		X			
Review advice from work areas e.g. human resources, finance and information technology on incidents where there was a breakdown in internal controls. Consider standing reports from CFO, CIO and HR on key risks, issues and incidents at each meeting except the financial statement meeting.	X				X
Consider how findings in internal audit and OAG audit reports impact on the entity's internal controls.		X	X		
Satisfy itself that management periodically assesses the adequacy of information security arrangements.		X			
Review whether appropriate policies and procedures are in place for the management and exercise of delegations.		X			
Review the assurance map.	X				X
Review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour.	X				
4. Compliance and ethics					
Review the effectiveness of processes to monitor compliance with relevant laws and regulations.	X				X
5. Internal audit					
Review the proposed internal audit plan for the next financial year, ensuring the coverage is aligned with key risks and recommend approval of the internal audit plan by the accountable authority.		X			
Review progress of the internal audit plan.	X	X		X	X
Review internal audit reports and provide advice to the accountable authority on significant issues identified and actions required.	X	X	X	X	X
Review the implementation status of internal audit recommendations.	X	X	X	X	X

(Appendix AAR: 8.1D)

Functions, responsibilities and associated activities	Mar	Jun	Aug	Sept	Dec
Review the <i>Internal Audit Charter</i> to ensure appropriate authority, access and reporting arrangements are in place.	X				
Review the performance of internal audit.				X	
Advise the accountable authority on the adequacy of internal audit resources and budget to carry out responsibilities, including completion of the audit work plan.	X				
Meet privately with the Chief Audit Executive.	X				
Provide advice to the accountable authority on the appointment of internal audit service providers (if applicable).		X			
6. Financial reporting					
Receive advice on changes in accounting standards, legislation, and regulations.	X	X		X	X
Review progress in preparing the financial statements against the preparation plan/timetable.	X	X			
Review briefing from management on significant emerging issues, judgements and estimates impacting the financial statements. Review accounting policy papers on key matters prior to management's provision to OAG.		X			X
Review financial management reports, where required.	X		X		X
Review of financial statements including:			X		
<ul style="list-style-type: none"> • consistency with members' understanding and knowledge of the entity 			X		
<ul style="list-style-type: none"> • review compliance with accounting standards, <i>Financial Management Act 2006</i>, <i>Treasurer's Instructions</i>, <i>Local Government Act 1995</i> and relevant regulations 			X		
<ul style="list-style-type: none"> • review the appropriateness of accounting policies including any significant changes in policies 			X		
<ul style="list-style-type: none"> • review areas subject to significant judgement and/or estimates 			X		
<ul style="list-style-type: none"> • review significant or non-routine transactions 			X		
<ul style="list-style-type: none"> • review the CFO certification in relation to the quality of the financial statements, internal controls and compliance (State government entities) 			X		

(Appendix AAR: 8.1D)

Functions, responsibilities and associated activities	Mar	Jun	Aug	Sept	Dec
<ul style="list-style-type: none"> review draft management representation letter 			X		
<ul style="list-style-type: none"> review whether management has addressed issues raised by the OAG including financial statement adjustments or revised disclosures 	X	X	X	X	X
<ul style="list-style-type: none"> discuss the adequacy of the entity's accounting policies and quality of processes for preparing the financial statements with the OAG 			X		
<ul style="list-style-type: none"> draft the advice to the accountable authority recommending the signing of the financial statements and management representation letter. 			X		
Discuss lessons learned from the current year financial statement process and the proposed strategy and timetable for next year.					X
Review the processes for ensuring that financial information included in the annual report is consistent with the audited financial statements.			X		
7. Performance reporting (mainly State government entities)					
Review systems and procedures for developing, measuring and reporting the entity's key performance indicators.		X	X		
Review the key performance indicator results and associated disclosures to ensure they are reasonable, clearly disclosed and consistent with financial and other information about the entity's performance.			X		
Review whether key performance indicators are consistent with members' understanding and knowledge of the entity.					
Ensure that there are adequate documentation and records to support the measurement of key performance indicators.		X	X		
8. External audit (OAG)					
Discuss OAG audit planning summary for financial audits.	X				
Receive OAG updates on issues arising from financial or performance audits.	X	X	X	X	X
Review the OAG interim management letter for the financial audit and assess the appropriateness of management's responses to recommendations.			X		
Discuss OAG exit brief and final management letter for				X	

(Appendix AAR: 8.1D)

Functions, responsibilities and associated activities	Mar	Jun	Aug	Sept	Dec
the financial audit and assess the appropriateness of management's responses to recommendations.					
Review the status of implementation of OAG financial and performance audit recommendations.	X	X	X	X	X
Review form and content of the OAG draft audit report.			X		
Satisfy itself that the appropriate mechanisms are in place to review and implement, where appropriate, issues raised in OAG better practice guides and performance audits of other State and local government entities.	X				
Meet annually with OAG without management present.				X	
9. Committee operations					
Provide a report to the accountable authority on audit committee operations and activities.					X
Conduct an assessment of the performance of the audit committee and ensure that the committee complies with its charter.					X
Agree on the annual work plan; and set priority areas for the coming year.	X				
Review the audit committee charter and recommend any substantive changes to the accountable authority.	X				

Auditor General's reports

Report number	2019-20 reports	Date tabled
25	WA's Transition to the NDIS	18 June 2020
24	Opinion on Ministerial Notification	16 June 2020
23	Opinion on Ministerial Notification	29 May 2020
22	Regulation of Asbestos Removal	21 May 2020
21	Audit Results Report – Annual 2019 Financial Audits	12 May 2020
20	Local Government Contract Extensions and Variations and Ministerial Notice Not Required	4 May 2020
19	Control of Monies Held for Specific Purposes	30 April 2020
18	Information Systems Audit Report 2020 – State Government Entities	6 April 2020
17	Controls Over Purchasing Cards	27 March 2020
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019

(Appendix AAR: 8.1D)

Report number	2019-20 reports	Date tabled
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

 @OAG_WA

 Office of the Auditor General for
Western Australia

Western Australian
Auditor General's Report



**Information Systems
Audit Report 2020 –
Local Government
Entities**

Office of the Auditor General
Western Australia

Audit team:

Jordan Langford-Smith
Kamran Aslam
Walber Almeida
Karla Cordoba
Fareed Bakhsh
Nomin Chimid-Osor

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

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

© 2020 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISSN: 2200-1913 (Print)
ISSN: 2200-1921 (Online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Information Systems Audit Report 2020 –
Local Government Entities**



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

INFORMATION SYSTEMS AUDIT REPORT 2020 – LOCAL GOVERNMENT ENTITIES

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

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

I wish to acknowledge the assistance provided by the staff at the entities included in our audits.

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

CAROLINE SPENCER
AUDITOR GENERAL
25 June 2020

Contents

Auditor General’s overview.....	2
Information systems – security gap analysis	3
Introduction	4
Conclusion	4
Background	4
What we found	5
Recommendations	10
General computer controls and capability assessment results for local government entities	11
Introduction	12
Conclusion	12
Audit focus and scope	13
What we found	14
Recommendations	23
Appendix 1 – Better practice guidance to manage technical vulnerabilities	24

Auditor General's overview

I am pleased to present our first local government Information Systems Audit report since the proclamation of the *Local Government Amendment (Auditing) Act 2017*. The report summarises the results of the 2019 cycle of information systems audits at 10 local government entities.



Our general computer control audits are a fundamental part of our financial audits. They help to provide assurance that the financial information generated by information systems is accurate, reliable and completely recorded. While local governments will differ in the size and scale, it is critical that they have effective controls to manage information systems.

The report has 2 parts:

- Information systems – security gap analysis
- General computer controls and capability assessment of local government entities.

The security gap analysis benchmarks the results of local government entities' security practices against a globally recognised standard. This standard provides a set of controls which entities can easily implement to protect critical information from internal and external threats. The standard provides useful guidance on how entities can address weaknesses and risks to their information security. My Office performed a similar exercise for State government entities in our 2013 Information Systems Audit Report.

We found that all 10 local government entities had significant shortcomings in their information security practices. Entities need to seriously consider these standards and the recommendations in this report to improve information security practices and protect the confidentiality, integrity and availability of information and systems.

The second part of this report outlines the results of our general computer controls audits and capability assessments. Overall, the level of maturity in the reviewed local government entities was low, with no entity meeting our minimum benchmark across all control categories.

Local government entities' information systems are integral for delivering key public services. However, most of the entities do not have a holistic view of activities that pose risks to their information systems. Entities should have visibility over their systems and take a strategic approach to address these risks.

International standards provide a good framework and starting point for entities to develop and implement sound practices in their operational and strategic security processes. My Office will continue to monitor and report on general computer controls and capability assessments of local government entities. We expect to see better results similar to the improvements made in the State sector in recent years as reported through our regular information system audit program.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information systems – security gap analysis

Introduction

The objective of this security gap analysis was to determine whether local government entities are adopting adequate controls in managing their information security. We assessed the information security controls at 1 regional and 9 metropolitan local government entities of varying size to determine whether they met the requirements of International Security Standard 27002 (AS ISO/IEC 27002:2015). This standard provides a framework and set of controls to ensure IT environments are managed to preserve the confidentiality, integrity and availability of information. Most of these controls are globally recognised as good practice and require minimal effort to implement.

Conclusion

All audited entities had significant gaps in their management of information security when compared against the standard. We found that entities did not have good practices to manage information and cyber security. Entities did not have appropriate policies and processes to identify and guide information security practices and they often lacked ongoing monitoring processes to detect and respond to threats. These gaps in security controls seriously undermine the confidentiality, integrity and availability of information held by these entities.

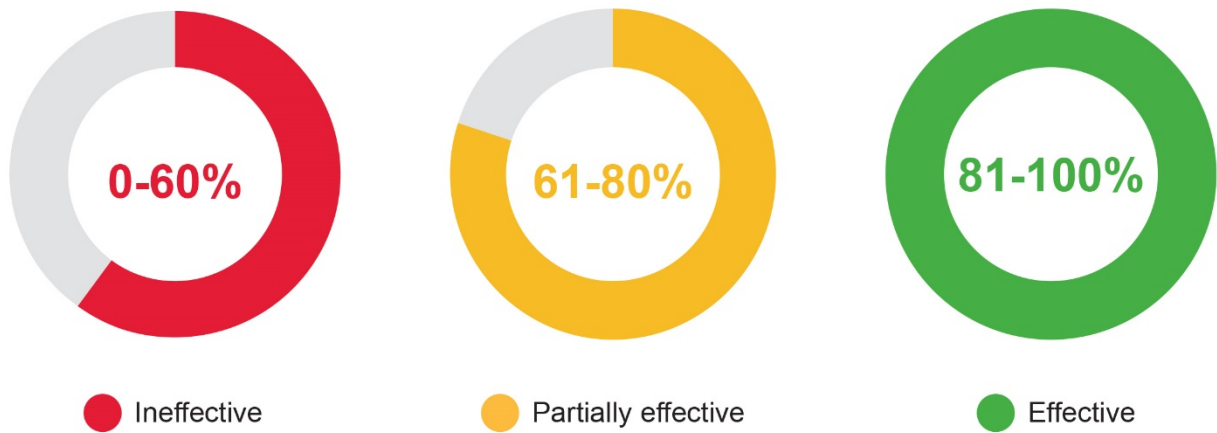
Background

Local government entities hold information, including confidential information about people and the community, which is fundamental to their operations and should be protected from external and internal threats. As IT systems and computing environments become more interconnected, the amount of information grows, along with the number and diversity of threats. Effective information security involves managing people, processes and technology to preserve the confidentiality, integrity and availability of information.

Entities can use the information security standard as a starting point to develop sound practices, or to assess their current controls. The standard has 14 areas with each area containing various controls that can be tailored to needs, size and complexity of entities.

In order to determine an overall rating for each area, we:

- determined which controls were applicable
- assessed and gave individual controls a score
- consolidated these scores to calculate an overall result which considered the number of effective controls in the area
- rated scores above 80 percent to be effective, scores from 61 to 80 percent as partially effective, and below 61 percent as ineffective.



Source: OAG

Figure 1: Scale to score entity controls

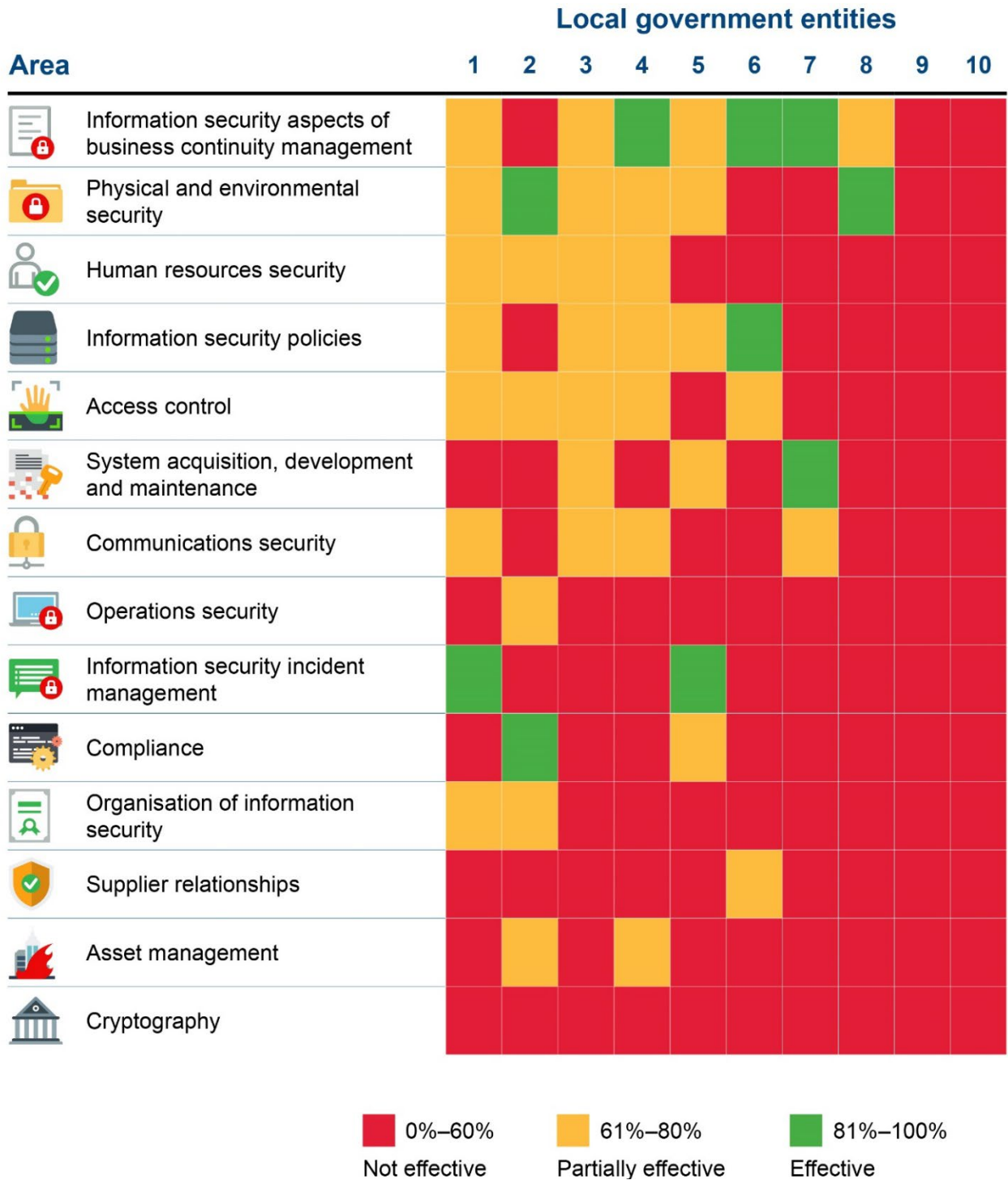
We evaluated if entities were effectively meeting information security best practices by comparing their controls against the 14 areas of the ISO 27002 standard. In performing this work, we also assessed if:

- entities had identified and defined the security requirements based on risks to their information systems
- appropriate controls were in place to mitigate information security risks
- mitigating controls were in place where practices did not align with international standards.

What we found

All of the audited entities had significant gaps in meeting the good practice standard across several control areas (Figure 2). Only 4 entities demonstrated that they were effective, or partially effective in at least 7 of the 14 areas. In order to protect the security of the information and systems of the audited entities, we have not named them in this report. We provided each audited entity with a copy of their gap analysis results.

(Appendix AAR: 8.1E)



Source: OAG

Figure 2: Results of security gap analysis for 10 local government entities

Each entity has unique security requirements based on their business needs. However, the majority of the entities had not assessed and identified their security requirements. Generally, security requirements can be identified through:

- assessing risks, taking into account the overall business strategy and objectives including vulnerabilities and threats to assets
- understanding legal, statutory and contractual requirements that apply to the entity and its contractors and service providers

(Appendix AAR: 8.1E)

- understanding the set of principles, objectives and business requirements for information handling to support operations.

Security policies did not provide direction and support for information security

Half of the entities did not have adequate policies outlining their approach for managing information security objectives. We found that policies did not contain guidance for key areas, including:

- roles and responsibilities for information security management
- access management
- protection from malware or malicious code
- use of IT assets and technical vulnerability management.

It is critical that entities take a strategic approach to information security by understanding the risks and implementing appropriate policies for the governance of security.

Additionally, none of the entities had a policy or a management approach on the use of cryptography controls, with all 10 entities rated as ineffective. A lack of guidance or direction for cryptography controls increases the risk that the confidentiality and integrity of information held by these local government entities could be compromised.

We also found 90% of the entities did not have good processes to check compliance with security requirements. For example, performing periodic internal reviews is a good way to ensure controls are working as expected. Without processes to detect policy breaches and non-compliance, entities cannot determine if their controls are operating effectively.

Poor controls risked network and operations security

Nine of the 10 entities did not have good practices to manage operational security. Without good practices, entities are at greater risk that internal and external threats will compromise their systems.

Operational security deals with day-to-day activities related to information processing and communication facilities. The weaknesses we found in controls over network and operations security included:

- a lack of change management processes. Changes may inadvertently introduce risks if they are not appropriately managed and tested prior to implementation
- network security appliances are not securely managed as they use insecure protocols. Insecure protocols that exchange information in plain-text can be used to compromise networks
- firewall events are only retained for limited periods and staff use shared generic accounts to administer firewalls. This makes it difficult to investigate and hold malicious users accountable as actions cannot be linked to them
- there were no processes to adequately assess and remediate security weaknesses. These weakness could be exploited to gain unauthorised access to entity systems and information
- a lack of controls to observe and review network activities. This could result in unauthorised or malicious activity going undetected
- data backup plans did not reflect current IT infrastructure. Also, entities were not testing the integrity of data on backups. Without appropriate backups and testing, entities risk

(Appendix AAR: 8.1E)

permanent data loss and may not be able to deliver their core services if systems or information are compromised

- inadequate segregation of networks. Weaknesses in a part of the network may enable malicious actors to access the entire network
- anti-malware controls were not installed on key servers. This could result in malware infections and compromise of systems and critical information.

Most entities had business continuity strategies but few had tested these

Three entities in the sample had good practices to manage business continuity and information security aspects during disaster situations. Four entities had not verified their capability to recover and ensure security of information during a serious interruption, and only partially met the standard. It is crucial to have well developed and verified business continuity and recovery strategies that address the security of information in crisis situations.

The remaining 3 entities had not adequately defined the information security requirements and plans in a disaster situation and consequently had inadequate business continuity and recovery strategies. This meant that a disaster or pandemic could disrupt their key services for prolonged periods and potentially compromise information security.

Poor access management controls resulted in inappropriate access

Half of the entities did not have good processes to manage access to systems and networks. The remaining half had partially effective controls to manage access. Some of the weaknesses we found include:

- a number of former staff still had access to systems. We found instances where systems were accessed inappropriately by former employees without an adequate explanation
- no formal process was in place to request and authorise access to systems
- weak password and authentication controls
- a lack of processes to review user access and privileges.

These control weaknesses significantly exposed entities to unauthorised access to systems and information.

Entities risked not effectively responding to security incidents

Only 2 entities had an appropriate plan to manage information security incidents. The remaining 8 entities did not have response plans, awareness programs and procedures for detecting security incidents and handling of forensic evidence to effectively manage security incidents. These controls are important to detect and appropriately respond to security incidents. Without robust and effective processes for responding to and managing security incidents, entities could face extended service outages and reputational damage in the event of an incident.

Information was at risk due to inadequate supplier management controls

The majority of the audited entities did not document or demonstrate their understanding of information security risks associated with the use of suppliers or contractors. Entities regularly employ contractors or procure systems to deliver key services. As part of this process, they may allow contractors to access information or store data on contractor managed systems. Even if entities use contractors, they are responsible for protecting their

(Appendix AAR: 8.1E)

information and managing how it is used. Understanding vendors, their security posture, services and systems is vital in maintaining effective information security controls.

Only 1 entity had partially effective controls to manage supplier risks. Without these controls there is an increased risk that entity information is exposed to unauthorised access and disclosure. In addition, by not embedding information security controls and practices into arrangements with suppliers and contractors, entities may have limited recourse in the event of an information security incident.

Physical and environmental security could be improved

Two entities met good practice standards in this area and 4 entities had partially effective controls. The remaining 4 entities were not managing the physical and environmental controls well. These entities have not formally defined the roles and responsibilities for managing the server room and their physical access controls were not operating effectively. For example, fire suppression systems were not installed, an excessive number of staff had access to server rooms, and access was not monitored. These weaknesses could result in unauthorised access to assets and accidental or deliberate damage to systems and information.

Information security controls were not considered over the lifecycle of information systems

Seven entities did not have good practices for managing their information and IT assets over the lifecycle of information systems. In particular, these entities did not have adequate plans and procedures to manage the acquisition, maintenance, disposal and re-use of IT and information assets. It is important to identify all assets that process information to ensure these are appropriately protected and the information on the assets cannot be inappropriately accessed, even after disposal.

We found that the majority of the entities had not defined how to classify information based on its value, legal requirements, criticality and sensitivity. As a result, appropriate security controls were not applied to information and assets based on these factors, increasing the risk to sensitive information.

Inadequate human resource security controls could threaten information security

Six entities did not have effective controls to ensure that information security risks were appropriately managed when staff were hired or terminated. The remaining 4 entities only had partially effective controls. Some of the weaknesses we identified include:

- no defined requirements for background checks before employing staff and contractors
- confidentiality and non-disclosure agreements not required for new staff
- inadequate induction and ongoing programs to inform staff and contractors of their information security responsibilities.

People play a fundamental role in maintaining information security. It is crucial that suitable people are hired, staff understand their responsibilities for information security and that the security of information is managed properly when staff leave the organisation. Poor practices for managing staff increase the risk of information or systems being compromised.

Recommendations

Local government entities should:

1. understand and assess the risks unique to their business activities and environment to inform their strategy for information security management
2. assess their controls against good practice standards to identify gaps and develop plans to improve information security. Entities can seek further guidance from other good practice standards. For instance, the Australian Cyber Security Centre maintains the *Australian Government Information Security Manual*¹ to assist entities in protecting their information and systems. The National Institute of Standards and Technology publishes *NIST Cybersecurity Framework*² to help organisations improve the management of cybersecurity risks
3. implement processes to continuously monitor and improve information security controls to ensure they meet entity needs.

Under section 7.12A of the *Local Government Act 1995*, the 10 audited entities are required to prepare an action plan addressing significant matters relevant to their entity for submission to the Minister for Local Government within 3 months of this report being tabled in Parliament and for publication on the entity's website. This action plan should address the points above, to the extent that they are relevant to their entity.

¹ <https://www.cyber.gov.au/ism>

² <https://www.nist.gov/cyberframework>

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**General computer controls and capability
assessment results for local government entities**

Introduction

In 2018-19, we audited the general computer controls (GCCs) at a sample of 1 regional and 9 metropolitan local government entities. Our GCC audits are integral to our annual financial audits of local government entities as they help to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems needed for annual financial reporting.

Information systems underpin most aspects of local government operations and services. It is important that entities implement appropriate controls to maintain reliable, secure and resilient information systems. These controls are equally important in smaller local government entities who may not have a dedicated IT department or staff, but may rely on contractors to provide the necessary support.

We use the results of our GCC work to inform our capability assessments of entities. We asked entities to self-assess their capability maturity across the 6 control categories using our assessment criteria. We then met with each of the entities to compare their assessment with ours, which was based on the results of our GCC audits.

Capability maturity models (CMMs) are a way to assess how well-developed and capable entities' established IT controls are. The model provides a benchmark for entity performance and a means for comparing results from year to year, and across entities.

The model we have developed uses accepted industry good practice as the basis for assessment. Our assessment of GCC maturity is influenced by various factors including the:

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

We focused on the following 6 categories to determine the maturity of entity control environments:



Source: OAG

Figure 3: GCC categories

Conclusion

All 10 local government entities need to improve their general computer controls. We reported 150 control weaknesses across the 10 entities, with 13 of these weaknesses rated

as significant. As these weaknesses could significantly compromise the confidentiality, integrity and availability of information systems, the local government entities need to act promptly to resolve them.

Our capability assessment results show that none of the entities met our expectations across all control categories. We found weaknesses in controls for information security, business continuity, change management, physical security and IT operations, with many entities falling below our benchmark. Whilst some entities had good IT risk policies, others need to improve how they identify and treat information risks.

Audit focus and scope

We conducted GCC audits and capability assessments at 10 local government entities. We used a 6 point rating scale³ from 0 to 5, detailed in Figure 4, to evaluate each entity's capability maturity level in each of the GCC categories. The model provides a reference for comparing entity results from year to year. We expect entities to achieve a level 3 (Defined) rating or better across all the categories.



Source: OAG

Figure 4: Rating scale and criteria

³ The information within this maturity model assessment is derived from the criteria defined within COBIT 4.1, released in 2007 by ISACA.

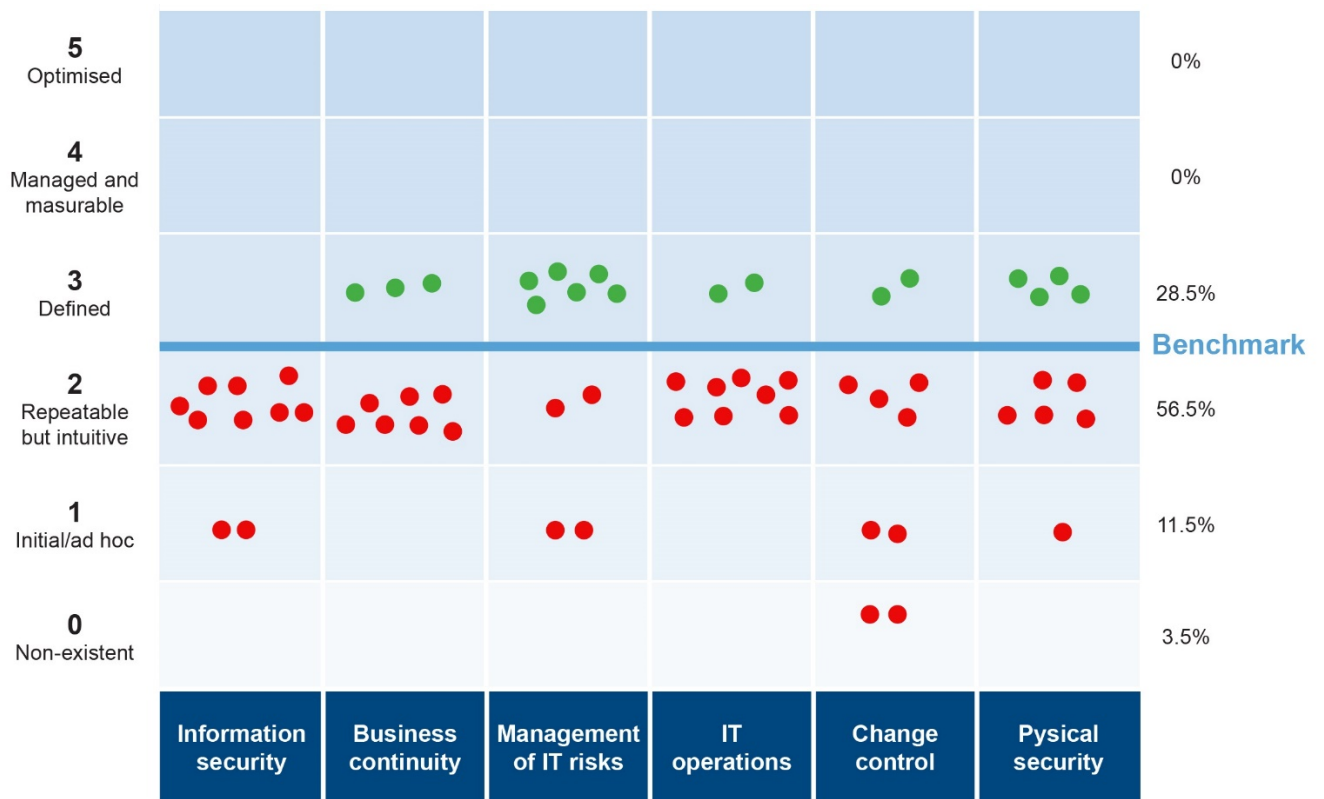
What we found

Capability maturity model assessment results

None of the local government entities we reviewed met our expectations across all control categories.

Entities did not have adequate controls to effectively manage information security, change management, IT operations, physical security and continuity of business. Poor controls in these areas left systems and information vulnerable to misuse and could impact critical services provided to the public. We have included specific case studies that provide more detail where we identified weaknesses in controls that could potentially compromise entities' systems.

Figure 5 shows the results of our capability assessments across all 6 control categories for the 10 entities we assessed.



Source: OAG

Figure 5: Capability maturity model assessment results

Information system controls

We reported information system control weaknesses identified during our GCC audits to local government entities in management letters. We identified 150 GCC control weaknesses across 10 entities, with 9% of the weaknesses rated as significant requiring prompt action, 75% as moderate which should be addressed as soon as possible, and the remaining 16% as minor. Nearly half of all issues were about information security which was also the category that had most of the significant findings.

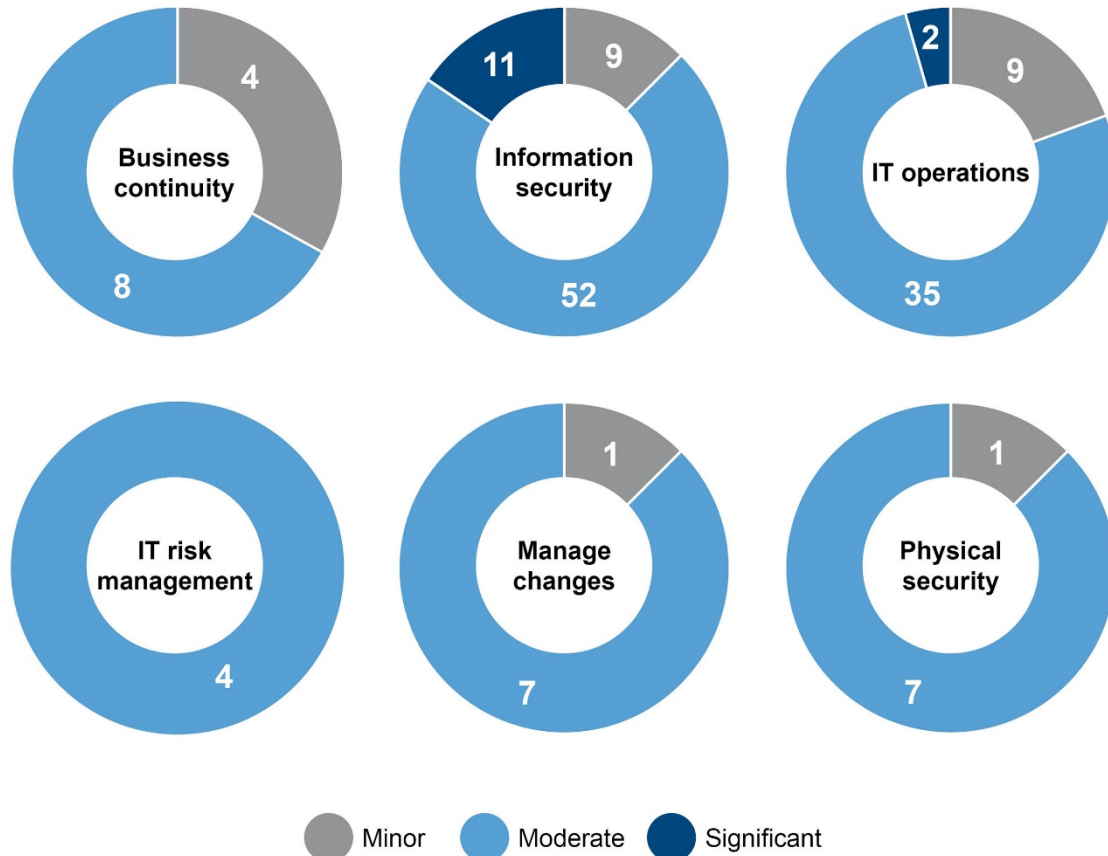
Management letters issued to entities contained all the findings. However, we removed sensitive technical details which, if made public, could increase the risk of cyber-attacks for

(Appendix AAR: 8.1E)

those entities. We reported these details separately through confidential letters to each local government entity to assist them in addressing the weaknesses. Entities generally agreed to implement the recommendations included in our management letters.

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

While the majority of our findings are rated as moderate, a combination of these issues can leave entities with more serious exposure to risk.



Source: OAG

Figure 6: Distribution of ratings for GCC findings in each control category we reviewed

Information security

Good information security practices are critical to protect the information held in key financial and operational systems from accidental or deliberate threats and vulnerabilities.

We found that all 10 local government entities need to improve their practices for managing information security, with no entity meeting our benchmark. We reported 72 issues, nearly half related to the security of information and systems. It is concerning that 11 were rated as significant requiring prompt attention, as they seriously exposed the entity's systems and information to misuse.

Several entities had not clearly defined roles and responsibilities for information security. This, coupled with a lack of appropriate policies and practices, meant their approach towards security was inconsistent and ad-hoc.

A common weakness we found at most entities was a lack of processes to identify and patch security vulnerabilities in systems and ICT infrastructure. Our vulnerability scans of key entity systems identified a range of critical and high severity vulnerabilities which had not been

(Appendix AAR: 8.1E)

patched. These left the systems open to compromise. Our better practice guidance at Appendix 1 provides practical information to help entities manage their vulnerabilities.

The following case studies were selected to highlight the risks to entity information from systems not regularly being patched and inadequate access controls, including remote access.

Information and systems are at risk due to inadequate vulnerability management

One of the audited entities did not have appropriate processes to identify and patch security vulnerabilities leaving systems vulnerable to exploitation through unauthorised and inappropriate access. Weaknesses included:

- The entity did not perform regular vulnerability assessments to identify and address weaknesses in a timely manner.
- It also did not have a process to identify vulnerable devices or computers on the network. It is extremely important to have visibility over devices connected to the network, and their vulnerabilities. Our scans identified an unmanaged computer on the network which was still susceptible to well-known critical software vulnerabilities including EternalBlue, Petya and Bluekeep. Patches to address EternalBlue and Petya vulnerabilities were released by mid 2017.
- Over 340 critical and 1500 high severity vulnerabilities on a sample of 50 servers and workstations.
- The entity's security update processes did not include core network devices such as firewalls, routers and switches, leaving them outdated and exposed.

Without an effective process to identify, assess and address relevant vulnerabilities in a timely manner, there is an increased risk that systems will not be adequately protected against potential threats. These vulnerabilities could be exploited and result in unauthorised access to IT systems and information.

Source: OAG

Figure 7: Poor vulnerability management leaves an entity exposed to cyber attacks

Excessive privileges and poor controls to manage infringements and rates could result in fraud

One entity we audited did not have adequate controls in place to manage its rates and infringement receipting system. We identified the following issues:

- A large number of users had excessive privileges to access system functions. For example, we found a number of users who had high level access to a range of functions including receipting, rates accounting and infringements.
- Generic accounts were used to process infringements and rate payments. These generic accounts did not require network authentication and bypassed security controls to access information and resources. In the event of error or wrongdoing, the entity would not be able to attribute responsibility to a particular user.
- Former staff still had infringement books assigned, used to issue fines to the public.
- There was no process to reconcile infringements that had been cancelled, or numbers in the fine sequence that had been skipped. The entity could not provide any information or reasons for cancelled infringements or the missing numbers. This basic control is fundamental to ensuring revenue is fully collected and there is no inappropriate issuance or cancellation of fines by current or former staff.
- There was no visibility to determine if users directly accessed or modified the infringement and rates system database. Infringements or rates notices could therefore be altered without an auditable trace or log.
- The servers for the infringement and rates system were not patched and were exposed to serious software vulnerabilities including EternalBlue and WannaCry.

When combined, these weaknesses could result in a person inappropriately modifying rates or infringement information, or receiving payments without processing them through the system. Due to the use of generic accounts not linked to any person and the lack of monitoring controls, it would be difficult for this entity to identify inappropriate or fraudulent transactions and activities, or investigate who is responsible. In addition, vulnerabilities in the system could be exploited to compromise the confidentiality, integrity and availability of systems.

Source: OAG

Figure 8: Lack of controls to manage the rates and infringement system

Poorly controlled remote access exposes entity's systems and information

One local government entity we audited provided remote access to its staff and contractors but did not have appropriate controls to manage associated risks.

We found:

- Staff and contractors used their personal devices to remotely connect to the entity network and systems. However, the entity had not defined the minimum security controls that these devices needed.
- We identified 6 external contractors with domain administrator privileges to the entity's network. Three of these contractors were not working on any active projects and 2 had not used their access in 4 years.
- Remote access system settings were not secured and publically exposed sensitive information such as the underlying operating system version and internal network information. This could be used by people with malicious intent to compromise the entity network and systems.
- The entity did not require multifactor authentication for remote access. This provides an additional layer of security to the remote system from unauthorised access attempts.
- The remote access infrastructure contained security misconfigurations, unsupported systems and missing patches. These weaknesses could be exploited to gain unauthorised access to the entity systems.

Source: OAG

Figure 9: Internet accessible systems lack controls

Business continuity

Good continuity planning helps ensure that key business functions and processes are restored promptly after a disruption. Business continuity and disaster recovery plans should be regularly tested. This minimises the risk of extended outages which could disrupt the delivery of important services.

We found that 7 of the 10 audited entities did not have up-to-date business continuity and disaster recovery arrangements in place. Some plans had not been updated since 2013 and may not reflect current business practices and IT infrastructure. As a result, in the event of a disruption or disaster, entities may not be able to restore and continue business processes and functions.

Weaknesses in business continuity and disaster recovery planning could have a serious impact on the critical services local government entities deliver to the public. To ensure business continuity, entities should have an up-to-date business continuity plan, disaster recovery plan and incident response plan. The business continuity plan defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the disaster recovery plan. The incident response plan needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response.

(Appendix AAR: 8.1E)

Management of IT risks

Six of the 10 local government entities we reviewed had good policies and procedures for managing IT risks. This was the control category where entities performed best. However, some common weakness at the other 4 included:

- a lack of risk management policies
- inadequate processes to review and report risks to senior management
- no risk registers for ongoing monitoring.

All entities should have risk management policies and practices that identify, assess and treat risks affecting key business objectives. Entities should be aware of the nature of risks associated with IT and have appropriate risk management policies and practices such as risk assessments, registers and treatment plans.

Without appropriate IT risk policies and practices, threats may not be identified and treated within reasonable timeframes. When risks are not identified and treated properly, entities may not meet their business objectives.

IT operations

Only 2 of the 10 entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. IT operations include day-to-day tasks designed to keep services running, while maintaining data integrity and the resiliency of IT infrastructure. In this area, we tested whether entities had formalised procedures and monitoring controls to ensure processes were working as intended.

Common weakness we found included:

- a lack of asset registers to track and monitor IT equipment which may lead to assets being lost or stolen and unintentional disclosure of information
- inadequate processes to ensure compliance with software licensing agreements. This could result in penalties for breaching licencing arrangements
- a lack of service level agreements with IT vendors and poor contract management practices leading to inadequate oversight of vendors or paying for services not provided
- inadequate retention and management of event logs. This means entities cannot track or identify malicious activities, nor they can investigate them
- a lack of access reviews which could result in inappropriate access.

Without appropriate IT strategies and supporting procedures, IT operations may not be able to respond to business needs and recover from errors or failures.

The following case studies highlight the risk to entities when devices and their events are not regularly monitored, and assets are not effectively managed.

No monitoring of inappropriate or malicious network activities

One entity had configured their network to log activities and events that occurred on their ICT infrastructure. However, there was no routine process to review those events.

The entity performed an informal review of logs and identified that a staff member had not complied with their acceptable use policies. Over a number of months, the staff member made several attempts (unsuccessfully) to access inappropriate websites featuring pornography. These websites are often carriers of malicious content and could put the entity's reputation at risk.

While it was good that there were controls in place to prevent access to inappropriate websites, and the entity took disciplinary action against the staff member, this case study highlights the importance of having formal processes for reviewing and monitoring logs to gain insights into inappropriate network activities. If proactive monitoring of important events is not in place, entities cannot detect any unauthorised or malicious activity or take timely corrective action. If it had not been for the informal review, the entity may not have identified inappropriate access attempts.

Entities can use centralised log management systems, such as Security Information and Event Management system, to analyse security events efficiently and effectively.

Source: OAG

Figure 10: Importance of regularly reviewing log events

Inadequate processes to manage IT assets

Another entity did not have appropriate processes to manage the lifecycle of IT assets. Issues we identified include:

- no policies relating to the disposal and re-use of assets
- computers donated to an external organisation without securely erasing data
- records of asset disposals were not maintained.

There is a high risk of unauthorised and unintentional disclosure of entity information if it is not securely removed from computers prior to disposal.

Source: OAG

Figure 11: Unauthorised disclosure of entity information

Insecure management of network devices

One local government entity did not manage its firewalls effectively. Issues we identified include:

- inappropriate firewall configuration which could allow external attackers to compromise the internal network
- individuals used shared generic accounts to administer the firewall which made it impossible to attribute actions to an individual
- backups of the firewall settings were not performed, leaving these vulnerable in the event of failure
- firewall security events were only retained for a short period (3 weeks) and alerts were not setup for critical events. This may make it difficult for the entity to detect or investigate security breaches, if required
- the firewall license for content filtering had expired, which allowed unrestricted access to all websites including those with inappropriate content.

The network and information systems are at a risk of compromise if network appliances are not managed appropriately.

Source: OAG

Figure 12: Increased risk of network compromise

Change control

We found that only 2 of 10 entities had appropriate processes to implement changes in their IT systems and infrastructure. We reviewed whether changes to systems were authorised, tested, implemented and recorded in line with management's intentions. Weaknesses we found included:

- a lack of formal system change management procedures. This increases the risk that changes, including those that may be harmful to systems and information, could be implemented without assessment
- no records of changes made to critical systems. This would make it difficult to investigate incidents that may have been caused by changes.

If changes are not controlled, they can compromise the security and availability of systems. As a result, systems will not process information as intended and entities' operations and services may be disrupted. There is also a greater chance that information will be lost and access given to unauthorised people.

We expected entities to have formal policies and procedures to ensure changes were risk assessed, tested, sufficiently documented and authorised prior to being implemented. This helps to ensure that changes to systems are consistent and reliable.

Physical security

Over half of the entities (6 of 10) did not have appropriate controls to protect their IT systems and infrastructure against environmental hazards and unauthorised access to server rooms. This means entities are at increased risk of unauthorised access and failure of information systems.

The following case study shows issues commonly faced by entities.

Server rooms are not well managed

At 1 entity, the primary server room was shared with the records area. All entity staff had access to this room and server racks were not locked. There was no fire suppression system or extinguishers installed in this area. Additionally, there were no controls to monitor the temperature or humidity of the server room.

Server rooms in shared areas present a risk of unauthorised access and outages due to deliberate or accidental damage to equipment. A lack of environmental controls in the server room, including fire management, could also result in system damage, malfunction due to heat or humidity and service outages.

Source: OAG

Figure 13: Information systems at risk of disruption

Recommendations

1. Information security

To ensure security strategies align with, and support, business objectives senior executives should implement appropriate frameworks and management structures.

Management should ensure good security practices and controls are implemented and continuously monitored.

2. Business continuity

Local government entities should have an appropriate business continuity plan, disaster recovery plan and incident response plan to protect critical services and systems from disruptive events. These plans should be tested on a periodic basis to ensure unexpected events do not affect business operations.

3. Management of IT risks

Local government entities need to identify threats and risks to their operations arising from information technology. These should be assessed and treated within appropriate timeframes. These practices should become a core part of business activities and have executive oversight.

4. IT operations

Local government entities should use good practice standards and frameworks as a reference to implement good controls for IT operations. Entities should have appropriate policies and procedures in place to manage incidents, IT risks, information security and business continuity.

Additionally, entities should ensure IT strategic plans and objectives support their overall business strategies and objectives.

5. Change control

Change control processes should be well developed and consistently followed when applying patches, updating or changing computer systems. All changes should be subject to thorough planning and impact assessment to minimise the occurrence of problems. Change control documentation should be current, and approved changes formally tracked.

6. Physical security

Local government entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental or environmental damage to computing infrastructure and systems.

Appendix 1 – Better practice guidance to manage technical vulnerabilities

Vulnerabilities are flaws in operating systems, devices and applications that attackers could exploit to gain unauthorised access to systems and information. Local government entities should have continuous monitoring processes to understand security weaknesses and gaps in their systems, devices and applications. Vendors generally provide patches to address flaws in applications and systems. Entities should implement appropriate processes and assign responsibilities to identify and treat these flaws.

The following table outlines some guiding principles entities should consider to address vulnerabilities. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre.⁴

Principle	Our expectation
Stocktake of assets	Entities should have visibility of all their ICT assets on the network including servers, workstations, printers, software applications, IoT and other network devices (switches, routers, firewalls).
Identify vulnerabilities	Regular vulnerability scans must be performed to identify security weaknesses. Where it is not possible to scan all assets at once, entities should prioritise and group assets to scan them in stages. Scans should be regular (e.g. continuous or monthly) as extended time gaps between scans leave the systems exposed for longer periods.
Understand the exposure	Each vulnerability poses a threat but some are more severe than others. Vulnerabilities generally have a severity rating based on impact and how easily they can be exploited. Entities should perform risk assessments to understand the exposure and take appropriate action.
Test and patch vulnerabilities	Entities should test patches before deploying them to live production systems. Ideally vulnerabilities should be patched as soon as possible, in line with their severity and impact levels. Entities should define appropriate timeframes to patch vulnerabilities based on their severity.
Apply mitigating controls if patching is not possible	In some instances, vulnerabilities cannot be addressed as they could affect the operations of a system (usually legacy systems), or a patch may not yet be available. Based on a risk assessment, mitigating controls should be applied with considerations to: <ul style="list-style-type: none">• virtual patches• segregating or isolating unpatched systems• upgrading systems that no longer receive security updates.

⁴ <https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches>

(Appendix AAR: 8.1E)

Principle	Our expectation
Don't forget the network devices – and printers	Network devices such as firewalls, routers and switches - and printers - are equally important. Vulnerability management processes must include them as well. Entities should regularly update the firmware and software for these devices.
Verify the patches	Entities should establish a process to verify that patches have successfully fixed the vulnerabilities. Some patches may fail to install or could require further configuration to fully address the weakness. Running another scan after applying patches can identify and report such instances.

Source: OAG

Figure 14: Better practice guidance to manage technical vulnerabilities

Auditor General's reports

Report number	2019-20 reports	Date tabled
26	Western Australian Public Sector Audit Committees – Better Practice Guide	25 June 2020
25	WA's Transition to the NDIS	18 June 2020
24	Opinion on Ministerial Notification	16 June 2020
23	Opinion on Ministerial Notification	29 May 2020
22	Regulation of Asbestos Removal	21 May 2020
21	Audit Results Report – Annual 2019 Financial Audits	12 May 2020
20	Local Government Contract Extensions and Variations and Ministerial Notice Not Required	4 May 2020
19	Control of Monies Held for Specific Purposes	30 April 2020
18	Information Systems Audit Report 2020 – State Government Entities	6 April 2020
17	Controls Over Purchasing Cards	27 March 2020
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019
4	Access to State-Managed Adult Mental Health Services	14 August 2019

(Appendix AAR: 8.1E)

Report number	2019-20 reports	Date tabled
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

 @OAG_WA

 Office of the Auditor General for
Western Australia

Western Australian Auditor General's Report



Regulation of Consumer Food Safety by Local Government Entities



Office of the Auditor General
Western Australia

Audit team:

Jordan Langford-Smith
Gareth Govan
Matthew Monkhouse
Lyndsay Fairclough

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

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

© 2020 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISSN: 2200-1913 (Print)
ISSN: 2200-1921 (Online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Regulation of Consumer Food Safety by Local
Government Entities**



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

REGULATION OF CONSUMER FOOD SAFETY BY LOCAL GOVERNMENT ENTITIES

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

Performance audits are an integral part of my Office's overall program of audit and assurance for Parliament. They seek to provide Parliament and the people of WA with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

This audit assessed whether local government entities effectively regulate consumer food safety in food businesses in their local area.

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

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

CAROLINE SPENCER
AUDITOR GENERAL
30 June 2020

Contents

Auditor General’s overview.....	2
Executive summary	3
Introduction	3
Background.....	3
Conclusion	5
Findings	6
Nearly 30% of high and medium risk food business inspections were overdue	6
Record management shortcomings have reduced LG entities’ ability to effectively regulate food businesses.....	7
LG entities did not always follow-up food safety issues consistently and enforce compliance	8
Recommendations	10
Response from local government entities.....	10
Audit focus and scope	11

Auditor General's overview

Local government entities (LG entities) are responsible for regulating food businesses in their local area. They ensure food businesses comply with the *Food Act 2008* and the *Australia New Zealand Food Standards Code* through a range of compliance activities such as food business inspections and enforcement actions. When food businesses are effectively regulated, the public can be more confident that the food they consume is safe.



This audit report focusses on the regulation of consumer food safety at 2 LG entities with a large number of food businesses such as restaurants, cafes and bars in their area. We found many inspections were overdue, recordkeeping was poor, and follow-up and enforcement was not always completed or consistent. These weaknesses increase the risk that unsafe food practices are not rectified, and the public consumes hazardous food.

The findings in the report are not about encouraging more regulation of businesses by LG entities, as this can lead to unnecessary burden on food businesses. Rather, the findings highlight the importance of a fair and equitable regulatory framework which focusses on the areas of highest risk to consumer safety. I am pleased that both LG entities generally agreed with the findings, and have advised that they are in the process of completing overdue inspections and improving their inspection and enforcement practices, and reporting.

Educating food businesses on safe food handling practices is an important part of the regulatory regime, and it was also pleasing to see examples of LG entities providing support to food businesses where there is a lack of knowledge, or where there is repeated non-compliance. However, it is also up to food businesses to make sure their staff understand and implement safe food handling practices. Ultimately, it makes good business sense to maintain clean premises and comply with food safety standards to avoid any reputational damage from serving food that makes people ill.

In the coming months I plan to report on the effectiveness of the Department of Health's (the Department) framework for monitoring consumer food safety. The Department was in the original scope of the audit, but my Office's work was put on hold as the Department was a frontline agency in the COVID-19 pandemic response. I'm looking forward to tabling this report as it will provide greater context and transparency as to how food safety is regulated in Western Australia.

I trust the findings in the report will help all LG entities with their compliance activities as food businesses continue to reopen in full, as a result of the easing of COVID-19 restrictions.

Executive summary

Introduction

This audit assessed whether local government entities (LG entities) effectively regulate consumer food safety in food businesses in their local area. It focused on inspection and enforcement processes at a metropolitan and a regional LG entity. These LG entities were selected because they have a large number of food businesses such as restaurants, cafes and bars, and were considered to provide a good baseline understanding of the risks and issues faced by LG entities and food businesses in relation to food safety regulation.

Due to the COVID-19 pandemic we amended the scope and size of the audit and decided to not identify the LG entities in the report.

Background

Food business regulation helps to reduce the number of food related diseases and ensure food is safe for consumption.¹ In 2016-17, Western Australia (WA) had over 23,000 registered food businesses. Across WA over 7,000 cases of intestinal infectious disease, such as salmonella, were reported in 2017.² The Department of Health (the Department) estimates that a 1% decrease in foodborne illness could save the community and health system nearly \$6 million annually.

In WA, the Department and LG entities are responsible for regulating food businesses. The *Food Act 2008* (the Act) and the Food Regulations 2009 (the Regulations) enable the Department and LG entities to inspect food businesses and enforce compliance with legislation and the *Australia New Zealand Food Standards Code* (the Standards). LG entities are responsible for food businesses in their district. Food businesses not in a district such as Rottnest Island and Kings Park, as well as hospitals and primary producers, are regulated by the Department.

To help make food safe for consumers, food businesses must meet specific requirements in the Standards (see examples in Figure 1).³ Some businesses are also required to have a food safety program which details how they manage high risk foods or vulnerable customers. For example, aged care facilities or restaurants selling uncooked seafood.

¹ Department of Health *Report on the Food Act 2008 (WA) – A report on the performance of the Food Act 2008 (WA) regulatory functions for the period 1 July 2013 to June 2016*.

² Not all of these cases were linked to food businesses.

³ This audit pre-dates the COVID-19 hospitality and tourism hygiene course requirements.

Australia New Zealand Food Standards Code

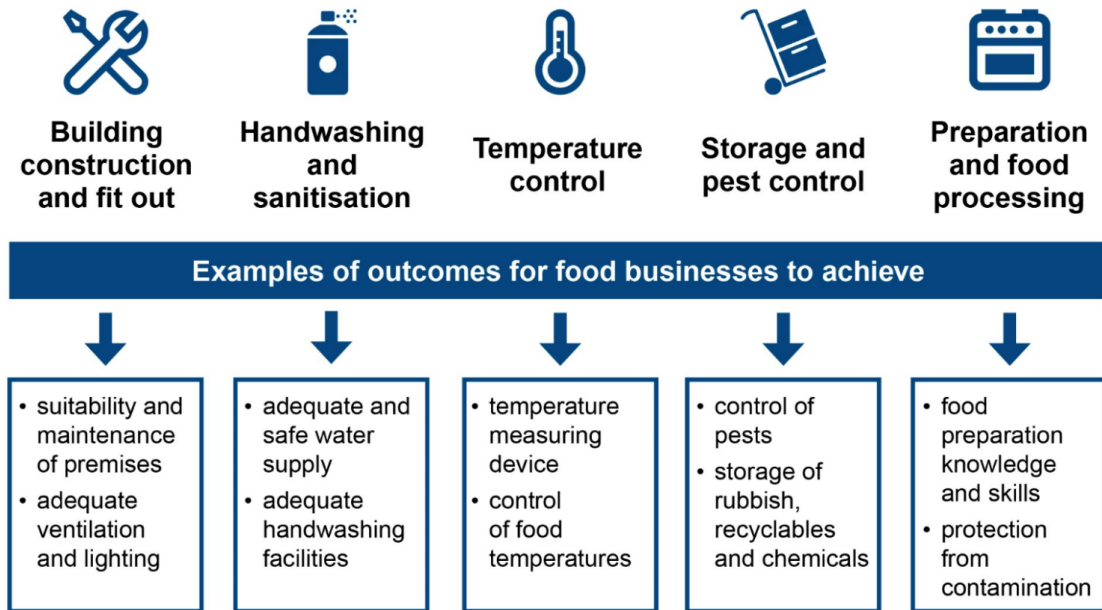


Figure 1: Examples of the Standards food businesses must meet

LG entities have environmental health officers (EHOs) to conduct food business registrations and inspections. EHOs assess each new food business and assign it with either a high, medium or low risk classification. This classification determines how often businesses are inspected. LG entities charge annual fees to recover the costs of these regulatory activities. EHOs also carry out other duties such as investigating noise complaints, hazardous waste assessments and event approvals.

The Australia New Zealand Food Authority (ANZFA) and the Department have developed better practice resources on the administration of food legislation. The guidance (as summarised in Table 1) helps ensure a consistent approach to business risk assessments and how often businesses are inspected. The starting point is the initial inspection frequency after a business is classified. Inspection frequency can be increased or decreased based on compliance history.

Risk classification	Inspection frequencies (every x months)		
	Starting point	Maximum	Minimum
Low	18	12	24
Medium	12	6	18
High	6	3	12

Source: Australia New Zealand Food Authority

Table 1: ANZFA inspection frequency model

EHOs can monitor and enforce food businesses' compliance with the Standards through education and training, follow-up inspections, improvement notices, infringements, prohibition orders or prosecution. Food businesses face fines of up to \$50,000 for an individual or \$250,000 for a body corporate if they are found not to comply with the Standards. EHOs often exercise discretion choosing which enforcement option to use to achieve compliance.

Conclusion

Current inspection and enforcement processes in the 2 audited LG entities do not support an effective risk-based approach for regulating food businesses.

While the 2 LG entities were conducting inspections, there were shortcomings in the compliance activities they used to regulate food safety in businesses. Many inspections were overdue, recordkeeping was poor, and follow-up and enforcement of compliance with food safety standards was not always consistent or completed. These shortcomings may lead to unsafe food practices going undetected or left unaddressed.

Both LG entities have advised that they are taking steps to complete overdue inspections and improve their inspection and enforcement practices and compliance reporting to address the audit findings.

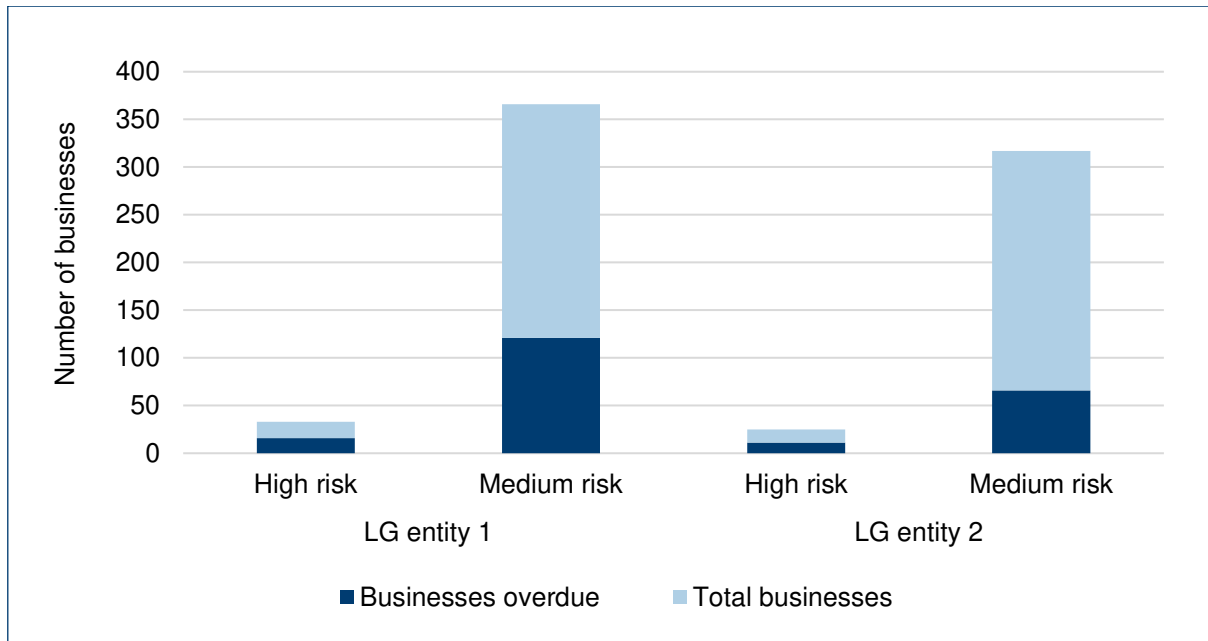
Findings

Nearly 30% of high and medium risk food business inspections were overdue

The 2 LG entities had not completed many required inspections. We found 214 of 741 high and medium risk food business inspections were overdue as at November 2019. When inspections are not completed according to risk, the LG entities are not checking that businesses comply with the Standards.

As LG entities did not have their own documented policy or approach to inspection frequency, we assessed inspections against the ANZFA starting point, the inspection frequency after a business is classified. Our analysis of high and medium risk business inspections (Figure 2) found:

- LG entity 1 had 48% of high and 33% of medium risk businesses overdue for inspection. On average, they were overdue by around 270 days
- LG entity 2 had 44% of high and 21% of medium risk businesses overdue for inspection. On average, they were overdue by more than 400 days.



Source: OAG, using information from the LG entities

Figure 2: Overdue high and medium risk business inspections by LG entity

LG entities have deviated from the better practice inspection frequencies and have not documented why. Therefore, they have less information about whether businesses are meeting food safety standards, increasing the risk that inadequate food practices are undetected. Additionally, businesses are paying annual fees for inspections not performed and they may miss out on receiving information and advice on their food safety practices.

Since being made aware of the findings, the LG entities advised that they were completing the overdue inspections. Both LG entities told us recently that some inspections could not be completed because businesses had cancelled their registration or were closed. One LG entity found some incorrect business risk classifications, which meant that an inspection was not due.

Record management shortcomings have reduced LG entities' ability to effectively regulate food businesses

Inspection and enforcement data was not well documented in the records systems at the 2 LG entities. We found instances where both LG entities had incomplete records of inspections and inaccurate business register data. We also found limited system functionality and compliance reporting. Quality records and reporting support good decision-making and help LG entities effectively and efficiently allocate limited resources.

In our sample of 35 Australian Food Safety Assessment (AFSA) paper inspection forms, we found examples where forms were difficult to read, missing details or an assessment against each standard was not recorded (Figure 3). EHOs need to complete these forms so non-compliance and inspection outcomes are clear to businesses and LG entities have correct records. Both LG entities acknowledged that there were issues with recording information and scanning the form. They advised us that they are developing an electronic form to improve the quality and completeness of inspection information. We note that there is an electronic version of the AFSA inspection form available.

AFSA Australian food safety assessment Office Copy

Business Name		Ref No		Scheduled	
Manager/Proprietor		Date	/ /	Follow Up	
Premises Address		Time		Complaint	
Business Phone		Officer		Other	

Indicate compliance using ✓/X in "Complies?" column. If non-compliance is serious indicate by also inserting a * in the "Serious N/C" column.

		Complies?	Serious N/C			Complies?	Serious N/C
Receiving				Recalls/Food Disposal			
1	Protection from contamination (5) of 3.2.2	✓		18	Food for disposal not sold/recall process (1, 12 of 3.2.2)	✓	
2	Identification/traceability of food (4) of 3.2.2	✓		Health, Hygiene & Knowledge			
3	Temperature control of PHF (5) and (6) of 3.2.2	✓		19	Health of food handlers - responsibilities (4 of 3.2.2)	✓	
Storage				Premises and Hygiene			
4	Protection from contamination (6) of 3.2.2	✓		20	Hygiene of food handlers - responsibilities (14, 15 of 3.2.2)	✓	
5	Appropriate environmental conditions (1) of 3.2.2	✓		21	Food business - responsibilities (14, 15 of 3.2.2)	✓	
6	Temperature control of PHF Inc frozen (6) of 3.2.2	✓		22	Adequate handwashing facilities (17 of 3.2.2 and 18 of 3.2.2)		
Processing				Food handling - skills & knowledge (1) of 3.2.2			
7	Safe and suitable food (7) of 3.2.2			23	Food handling - skills & knowledge (1) of 3.2.2		
8	Protection from contamination (7) of 3.2.2	✓		Premises and Hygiene			
9	Adequate cooking/processing (1) of 3.2.2	✓		24	Cleanliness of premises, fittings, equipment (13 of 3.2.2)	✓	
10	PHF out of temp. control for min. time (2) of 3.2.2	✓		25	Cleaning/sanitising of food contact surfaces (8 of 3.2.2)	X	
11	Cooling of PHF (7) of 3.2.2	✓		26	Suitability and maintenance of premises, fittings and equipment (21 of 3.2.2 and 21, 21, 1 & 12 of 3.2.2)	X	
12	Reheating of PHF (7) of 3.2.2	✓		27	Temperature measuring device (22 of 3.2.2)	X	
Display				Control of animals and pests (4) of 3.2.2			
13	Protection from contamination (8) of 3.2.2	✓		28	Use of "single use" items (23 of 3.2.2)	✓	
14	Temperature control of PHF incl. frozen (8) of 3.2.2	✓		29	Control of animals and pests (4) of 3.2.2	✓	
Packaging				Water supply adequate and potable (4) of 3.2.2			
15	Appropriate materials and process (9) of 3.2.2	✓		30	Water supply adequate and potable (4) of 3.2.2		
Transportation and Distribution				Disposal of sewage and waste water (5) of 3.2.2			
16	Protection from contamination (10) of 3.2.2			31	Disposal of sewage and waste water (5) of 3.2.2)		
17	Temperature control of PHF (10) of 3.2.2			32	Storage of refuse & recyclable matter (6 of 3.2.2)		
				Adequate ventilation and lighting (7 & 8 of 3.2.2)			
				Storage of personal effects/chemicals (18 of 3.2.2)			
				Adequate toilet facilities (16 of 3.2.2)			

COMMENTS/ACTION TO BE TAKEN

*- meat bags used to bag chicken in cool room & frozen
- meat, defrosted out of fridge
- cool room to be repaired keep temp history record
- meat & cow meat squirts*

Further Action?	N/A	Reinspection	Letter	Order/Notice	Explanation Notice	Reinspection date:
Serious N/C	Other N/C	Total N/C	Priority Classification	Circle - Increase/Retain / Decrease	Assessment Frequency	/ /
I have read and I understand the contents of this assessment.				Officer signature:		Officer contact No:
Signature of proprietor/staff:						

Source: OAG, using information from the LG entities

Figure 3: Example of an inspection form record

We found that business information stored in registers was not always accurate or complete. In particular:

- 47 of 1,204 businesses across both LG entities had no record of inspection in the registers
- 1 LG entity had 15 businesses in which the next inspection pre-dates the last inspection
- through a limited internet search by the OAG of 20 local businesses, 1 business was found to be operating but not known or registered by the LG entity. After we made the entity aware of this finding, they requested and received a registration application.

Incomplete or inaccurate information can result in missed inspections, and businesses not being inspected according to an appropriate risk classification.

Both LG entities had weaknesses in their risk assessment processes. One LG entity did not have supporting documentation for their business risk assessments, and advised that there were 24 high and medium risk businesses which had incorrect risk classifications. At the other entity, we found an instance where risk was not reassessed for a business after multiple items of serious non-compliance were identified. One of which was feeding cats in the kitchen. Inaccurate risk assessments can lead to businesses not being inspected appropriately or paying for more inspections than required.

The LG entities can also improve the way they manage and track inspections. Due to a system error at 1 LG entity, EHOs have to rely on setting reminders for follow-up inspections in their calendars to check non-compliance was resolved. We note 1 LG entity reports quarterly on inspections completed, while the other stopped similar reporting in November 2018, while they wait for a new system. Neither LG entity reported on inspections that were due or overdue. Compliance reporting provides management with oversight of inspections required and completed, and EHO workload.

Compliance information and data can also help identify systemic food safety issues, make decisions on education and support services, and determine appropriate enforcement options. Both LG entities have advised they are either conducting a review of their registers to identify other shortcomings or improving the accuracy and effectiveness of their register and compliance reporting.

LG entities did not always follow-up food safety issues consistently and enforce compliance

We found that the LG entities did not have adequate procedures to help EHOs determine which types of non-compliance require enforcement and follow-up, and when this should occur. While some compliance decisions may require the professional judgement and discretion of individual EHOs, it is important to have documented guidance to support consistent, risk based compliance actions.

Both LG entities were not following up instances of identified non-compliance in a consistent way, to ensure food safety issues were fixed. In our review of 41 inspections across both LG entities, there were 30 inspections that identified non-compliance in areas such as food skills and knowledge, cleanliness, maintenance, handwashing facilities and protecting food from contamination. We found:

- EHOs only recommended an improvement notice for 2 businesses, but these were never issued. One business had a follow-up inspection, while the other was later fined \$250 for hazardous foods that were being thawed with no temperature control.
- Five inspections completed by 1 LG entity identified between 11 and 20 separate items of non-compliance at each business but were enforced differently. Three of the

(Appendix AAR: 8.1F)

inspections required no further action, 1 resulted in a follow-up inspection, and the other was marked as requiring an improvement notice, but only had a follow-up inspection.

- Six businesses had follow-up inspections, but it was unclear if all items of non-compliance were fixed. One LG entity advised that non-compliance with a lower risk are often rectified at the time of inspection, but this wasn't always documented.

It is important for LG entities and other regulators to take consistent compliance actions for similar non-compliance. Clear and consistent enforcement processes and actions are equitable and make it easier for businesses to understand how LG entities assess and enforce compliance with the Standards.

We expected to see more formal enforcement processes used, based on the types of non-compliance found, but these were rarely used. According to Department records, in 2018-19, only 2.6% of 734 inspections across both LG entities resulted in formal enforcement. Less than 1% of all inspections resulted in an improvement notice, the first enforcement option for non-compliance. Under appropriate circumstances, formal enforcement actions send a clear and important message to businesses that their food safety practices need to be strengthened and is consistent with the Department's compliance and enforcement guidelines.

Recommendations

Local government entities should:

1. ensure food business inspections are prioritised and carried out according to their risk classification
2. ensure changes to inspection frequencies are only made based on a documented assessment of compliance history or other urgent requirement
3. improve recordkeeping for food business inspections and compliance reporting to:
 - a. better understand inspection and compliance history
 - b. identify compliance issues and follow-up activities
 - c. respond to emerging food safety issues
4. develop procedures and staff guidance to ensure non-compliant food businesses are followed up and Standards enforced in a consistent and timely manner
5. work with the Department of Health in the development and implementation of new electronic food safety inspection and recordkeeping systems.

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

Response from local government entities

Local government entities in our sample generally accepted the recommendations and confirmed that, where relevant, they will improve inspection and enforcement practices, recordkeeping and compliance reporting for regulating food businesses.

Audit focus and scope

This audit assessed if local government entities (LG entities) effectively regulate consumer food safety in food businesses. It focused on food business inspections, and enforcement of compliance with food safety legislation and the Standards at 2 LG entities. We did not attempt to detect non-compliance in food businesses.

In this audit we also examined how effectively the Department of Health monitors consumer food safety, inspects food businesses and enforces compliance. However, this part of the audit was put on hold due to the ongoing COVID-19 pandemic. We plan to table findings specific to the Department at a later date.

We reviewed practices for regulating food safety at 2 LG entities, including:

- food business registers containing 1,204 food businesses
- policies and procedures for regulating food businesses
- records and data on food businesses and regulatory activities
- inspection records and enforcement actions at food businesses from 2018 to 2019
- the timeliness and consistency of follow-up inspections and enforcement actions.

At each LG entity, we sampled 10 food businesses (5 high risk and 5 medium risk) from 2018 to 2019 to review risk assessments, any subsequent risk re-assessments, inspection records and any associated enforcement activities. We also accompanied an environmental health officer on a food business inspection at both LG entities.

We spoke with staff at the LG entities who deal with registration, risk assessment, inspection, education and enforcement of food businesses.

This audit did not review animal food processing premises, retail pet meat stores or businesses exempt from registration (such as newsagents selling low risk packaged foods).

This was a performance audit, conducted under Section 18 of the *Auditor General Act 2006*, in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other ethical requirements related to assurance engagements. Performance audits focus primarily on the effective management and operations of entity programs and activities. The approximate cost of undertaking the audit and reporting was \$184,000.

Auditor General's reports

Report number	2019-20 reports	Date tabled
27	Information Systems Audit Report 2020 – Local Government Entities	25 June 2020
26	Western Australian Public Sector Audit Committees – Better Practice Guide	25 June 2020
25	WA's Transition to the NDIS	18 June 2020
24	Opinion on Ministerial Notification	16 June 2020
23	Opinion on Ministerial Notification	29 May 2020
22	Regulation of Asbestos Removal	21 May 2020
21	Audit Results Report – Annual 2019 Financial Audits	12 May 2020
20	Local Government Contract Extensions and Variations and Ministerial Notice Not Required	4 May 2020
19	Control of Monies Held for Specific Purposes	30 April 2020
18	Information Systems Audit Report 2020 – State Government Entities	6 April 2020
17	Controls Over Purchasing Cards	27 March 2020
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

 @OAG_WA

 Office of the Auditor General for
Western Australia

RISK ASSESSMENT TOOL									
OVERALL RISK EVENT:		Review of Terms of Reference for the Audit and Risk Committee							
RISK THEME PROFILE:		8 - Errors, Omissions and Delays							
3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)									
6 - Engagement Practices									
RISK ASSESSMENT CONTEXT:		Operational							
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.	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 considering a review of the Terms of Reference would not be in line with the recommendations from the Auditor General's publication (Better Practice Guide).	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 adhering to the Auditor General's recommendation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	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.



AUDIT & RISK COMMITTEE

**INSTRUMENT OF APPOINTMENT
&
TERMS OF REFERENCE**

2019

By Resolution of Council
Ordinary Council Meeting 23/10/19
Resolution Number [309-19]



(Appendix AAR: 8.2B)

1	INTRODUCTION	1
2	NAME	1
3	OBJECTIVES – GENERIC.....	1
4	FUNCTIONS OF THE AUDIT AND RISK COMMITTEE.....	2
5	COMMITTEE OBJECTIVES - SPECIFIC	3
6	MEMBERSHIP	3
7	PRESIDING MEMBER.....	5
8	MEETINGS.....	6
9	QUORUM	7
10	DELEGATED POWERS	7
11	TERMINATION OF COMMITTEE	7
12	AMENDMENT TO THE INSTRUMENT OF APPOINTMENT AND DELEGATION.....	8
13	COMMITTEE DECISIONS	8
14	HISTORY OF COUNCIL RESOLUTION ESTABLISHING THE COMMITTEE	8
15	OFFICER(S) RESPONSIBLE FOR MANAGEMENT OF THE COMMITTEE	8

(Appendix AAR: 8.2B)

1 INTRODUCTION

The Council of the Shire of Dardanup (the "Council") establishes this committee under the powers given in Section 7.1A of the Local Government Act 1995, the committee to be known as the Audit and Risk Committee, (the "Committee").

The Council appoints to the Committee those persons to be members of the committee by resolution of Council. Membership of the Committee shall, unless otherwise specified, be for a term ceasing on the day prior to local government elections being held. Council may appoint members for a further term at the next available meeting following the elections.

The Committee shall act for and on behalf of Council in accordance with provisions of the Local Government Act 1995, local laws and the policies of the Shire of Dardanup and this instrument.

2 NAME

The name of the Committee is the "Audit and Risk" Committee.

3 OBJECTIVES – GENERIC

The following objectives are generic to all Council committees:

- 3.1 To consider, advise and assist the local government in performing specified functions or fulfilling required responsibilities within its district;
- 3.2 Where appropriate, to liaise with relevant agencies and other persons in the development, review and testing of Council policy and strategic objectives;
- 3.3 To carry out research and other activities as directed by the Council or prescribed by the regulations; and
- 3.4 To fulfil the objectives and/or undertake the specific tasks as a Committee of Council specified in Section 4 – Functions of the Committee and Section 5 Committee Objectives - Specific.
- 3.5 To ensure that all members dealings are carried out in accordance with the Shire of Dardanup Code of Conduct.

(Details of tasks to be endorsed by Council by resolution when the committee is established or as amended from time to time).

4 FUNCTIONS OF THE AUDIT AND RISK COMMITTEE

The detailed functions of the Committee are set out in the Local Government (Audit) Regulations 1996, Regulation 14, 16 and 17 as follows:

14. Compliance audits by local governments

- (1) *A local government is to carry out a compliance audit for the period 1 January to 31 December in each year.*
- (2) *After carrying out a compliance audit the local government is to prepare a compliance audit return in a form approved by the Minister.*
- (3A) *The local government's audit committee is to review the compliance audit return and is to report to the council the results of that review.*
- (3) *After the audit committee has reported to the council under subregulation (3A), the compliance audit return is to be —*
 - (a) *presented to the council at a meeting of the council; and*
 - (b) *adopted by the council; and*
 - (c) *recorded in the minutes of the meeting at which it is adopted.*

16. Functions of audit committee

An audit committee has the following functions —

- (a) *to guide and assist the local government in carrying out —*
 - (i) *its functions under Part 6 of the Act; and*
 - (ii) *its functions relating to other audits and other matters related to financial management;*
- (b) *to guide and assist the local government in carrying out the local government's functions in relation to audits conducted under Part 7 of the Act;*
- (c) *to review a report given to it by the CEO under regulation 17(3) (the **CEO's report**) and is to —*
 - (i) *report to the council the results of that review; and*
 - (ii) *give a copy of the CEO's report to the council;*
- (d) *to monitor and advise the CEO when the CEO is carrying out functions in relation to a review under —*
 - (i) *regulation 17(1); and*
 - (ii) *the Local Government (Financial Management) Regulations 1996 regulation 5(2)(c);*
- (e) *to support the auditor of the local government to conduct an audit and carry out the auditor's other duties under the Act in respect of the local government;*
- (f) *to oversee the implementation of any action that the local government —*
 - (i) *is required to take by section 7.12A(3); and*
 - (ii) *has stated it has taken or intends to take in a report prepared under section 7.12A(4)(a); and*
 - (iii) *has accepted should be taken following receipt of a report of a review conducted under regulation 17(1); and*
 - (iv) *has accepted should be taken following receipt of a report of a review conducted under the Local Government (Financial Management) Regulations 1996 regulation 5(2)(c);*
- (g) *to perform any other function conferred on the audit committee by these regulations or another written law.*

[Regulation 16 inserted: Gazette 26 Jun 2018 p. 2386-7.]

(Appendix AAR: 8.2B)

17. *CEO to review certain systems and procedures*

- (1) *The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to —*
 - (a) *risk management; and*
 - (b) *internal control; and*
 - (c) *legislative compliance.*
- (2) *The review may relate to any or all of the matters referred to in subregulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.*
- (3) *The CEO is to report to the audit committee the results of that review.*

5 COMMITTEE OBJECTIVES - SPECIFIC

The Audit and Risk Committee shall have the following objectives:

- 5.1 To meet with the auditor, once in each year and provide a report to Council on the matters discussed and outcome of those discussions;
- 5.2 Provide an effective means of communication between the external and internal auditors;
- 5.3 Examine the reports of the auditor to –
 - i.) determine if any matters raised require action to be taken by the local government; and
 - ii.) ensure that appropriate action is taken in respect of those matters;
- 5.4 Review annually the internal audit plan, including any reports produced as part of special assignments undertaken by internal audit.
- 5.5 To consider the Financial Management Systems Review required every three years under Regulation 5 of the *Local Government (Financial Management) Regulations 1996*, and report to Council the results of that review;
- 5.6 Consider and recommend adoption of the Annual Financial Report to Council.
- 5.7 To consider the Shire of Dardanup Risk Management Governance Framework and progress on the relevant action plans biannually.

Any variation to these objectives is not to be considered by the committee unless approved by Council.

6 MEMBERSHIP

- 6.1 The Council resolves to nominate no more than five elected members as members for the Committee for a period of two years or until the next

(Appendix AAR: 8.2B)

Ordinary Council election, the five elected members shall be members of the committee.

6.2 Membership as prescribed by the Local Government Act 1995 Section 7.1A is outlined below:

7.1A. Audit committee

- (1) *A local government is to establish an audit committee of 3 or more persons to exercise the powers and discharge the duties conferred on it.*
- (2) *The members of the audit committee of a local government are to be appointed* by the local government and at least 3 of the members, and the majority of the members, are to be council members.*

** Absolute majority required.*
- (3) *A CEO is not to be a member of an audit committee and may not nominate a person to be a member of an audit committee or have a person to represent the CEO as a member of an audit committee.*
- (4) *An employee is not to be a member of an audit committee.*

6.3 In addition to the above with regards to the specific membership of the Audit and Risk Committee the following sections in Local Government Act 1995, in relation to representation are also relevant:

5.10. Committee members, appointment of

- (1) *A committee is to have as its members —*
 - (a) *persons appointed* by the local government to be members of the committee (other than those referred to in paragraph (b)); and*
 - (b) *persons who are appointed to be members of the committee under subsection (4) or (5).*

** Absolute majority required.*
- (2) *At any given time each council member is entitled to be a member of at least one committee referred to in section 5.9(2)(a) or (b) and if a council member nominates himself or herself to be a member of such a committee or committees, the local government is to include that council member in the persons appointed under subsection (1)(a) to at least one of those committees as the local government decides.*
- (3) *Section 52 of the Interpretation Act 1984 applies to appointments of committee members other than those appointed under subsection (4) or (5) but any power exercised under section 52(1) of that Act can only be exercised on the decision of an absolute majority of the council.*
- (4) *If at a meeting of the council a local government is to make an appointment to a committee that has or could have a council member as a member and the mayor or president informs the local government of his or her wish to be a member of the committee, the local government is to appoint the mayor or president to be a member of the committee.*

5.11 Committee membership, tenure of

- (1) *Where a person is appointed as a member of a committee under section 5.10(4) or (5), the person's membership of the committee continues until —*
 - (a) *the person no longer holds the office by virtue of which the person became a member, or is no longer the CEO, or the CEO's representative, as the case may be; or*
 - (b) *the person resigns from membership of the committee; or*
 - (c) *the committee is disbanded; or*
 - (d) *the next ordinary elections day,*
whichever happens first.
- (2) *Where a person is appointed as a member of a committee other than under section 5.10(4) or (5), the person's membership of the committee continues until —*
 - (a) *the term of the person's appointment as a committee member expires; or*
 - (b) *the local government removes the person from the office of committee member or the office of committee member otherwise becomes vacant; or*
 - (c) *the committee is disbanded; or*
 - (d) *the next ordinary elections day,*
whichever happens first.

7 PRESIDING MEMBER

- 7.1 The CEO or delegated nominee will preside until the position of Presiding member is filled in accordance with Schedule 2.3 clause 3 of the *Local Government Act 1995*.
- 7.2 The Committee shall appoint a Presiding Member and Deputy Presiding Member to conduct its business in accordance with the following provisions of the *Local Government Act 1995*:

5.12 Presiding members and deputies, election of

- (1) *The members of a committee are to elect a presiding member from amongst themselves in accordance with Schedule 2.3, Division 1 as if the references in that Schedule —*
 - (a) *to "office" were references to "office of presiding member"; and*
 - (b) *to "council" were references to "committee"; and*
 - (c) *to "councillors" were references to "committee members".*
 - (2) *The members of a committee may elect a deputy presiding member from amongst themselves but any such election is to be in accordance with Schedule 2.3, Division 2 as if the references in that Schedule —*
 - (a) *to "office" were references to "office of deputy presiding member"; and*
 - (b) *to "council" were references to "committee"; and*
 - (c) *to "councillors" were references to "committee members"; and*
 - (d) *to "mayor or president" were references to "presiding member".*
- 7.3 The Presiding Member shall ensure that business is conducted in accordance with the Shire of Dardanup Standing Orders and that minutes of the proceedings are kept in accordance with Section 5.22 of the *Local Government Act 1995*.

5.22. *Minutes of council and committee meetings*

- (1) *The person presiding at a meeting of a council or a committee is to cause minutes to be kept of the meeting's proceedings.*
- (2) *The minutes of a meeting of a council or a committee are to be submitted to the next ordinary meeting of the council or the committee, as the case requires, for confirmation.*
- (3) *The person presiding at the meeting at which the minutes are confirmed is to sign the minutes and certify the confirmation.*

7.4 The Deputy presiding member has the following functions as per section 5.12 of the Local Government Act 1995:

5.13. *Deputy presiding members, functions of*

If, in relation to the presiding member of a committee —

- (a) *the office of presiding member is vacant; or*
- (b) *the presiding member is not available or is unable or unwilling to perform the functions of presiding member,*

then the deputy presiding member, if any, may perform the functions of presiding member.

7.5 A presiding member is to be chosen from the committee members present at the meeting if the presiding member or deputy presiding member are unavailable or unwilling to perform the functions of the presiding member in accordance with Section 5.14 the Local Government Act 1995:

5.14. *Who acts if no presiding member*

If, in relation to the presiding member of a committee —

- (a) *the office of presiding member and the office of deputy presiding member are vacant; or*
- (b) *the presiding member and the deputy presiding member, if any, are not available or are unable or unwilling to perform the functions of presiding member,*

then the committee members present at the meeting are to choose one of themselves to preside at the meeting.

8 MEETINGS

8.1 As there are no power or duty delegated to the committee the meetings are not open to the public.

8.2 The Committee shall meet on a quarterly basis, with a minimum of **4 meetings** per year, dates to be resolved by the Committee but generally February, May, September, December.

8.3 Notice of meetings including an agenda shall be given to members at least **5 days** prior to each meeting.

(Appendix AAR: 8.2B)

- 8.4 The Presiding member shall ensure that detailed minutes of all meetings are kept and shall, not later than **5 days** after each meeting, provide the members and Council with a copy of such minutes.
- 8.5 The minutes of the meeting are to be included in the next available Ordinary meeting of Council agenda for consideration of recommendations or to be received by the Council.
- 8.6 All members of the Committee shall have one vote. If the vote of the members present are equally divided, the person presiding is to cast a second vote.
- 8.7 Shire of Dardanup Local Law Standing Orders apply to all Shire of Dardanup committees.

9 QUORUM

- 9.1 Quorum for a meeting shall be at least 50% of the number of offices, whether vacant or not. A decision of the Committee does not have effect unless it has been made by a simple majority.

(Note – Council may, at the request of the Committee, agree to set the quorum at a lesser number. However in such circumstances any recommendation on expenditure of monies or on forming policy positions that is being made to Council or the CEO, the committee must have at least 50% of the members present to make a valid recommendation/s.)

10 DELEGATED POWERS

- 10.1 The Committee has no specific powers under the Local Government Act and is to advise and make recommendations to Council only.
- 10.2 The Council reserves the right to delegate powers to the committee if circumstances require delegation. The Delegation shall be recorded in the Council minutes prior to the delegation being exercised.

11 TERMINATION OF COMMITTEE

Termination of the Committee shall be:

- 10.1 In accordance with the Local Government Act 1995; or
- 10.2 At the direction of Council; or
- 10.3 On the specified date.

(Appendix AAR: 8.2B)

12 AMENDMENT TO THE INSTRUMENT OF APPOINTMENT AND DELEGATION

- 12.1 This document may be altered at any time by the Council on the recommendation of the Committee, or by direct resolution of Council.

13 COMMITTEE DECISIONS

- 13.1 Committee decisions shall not be binding on Council in any circumstance.
- 13.2 The decisions of the Audit and Risk Committee is to be by simple majority in accordance with Section 7.1C of the *Local Government Act 1995*:

7.1C. Decisions of audit committees

Despite section 5.20, a decision of an audit committee is to be made by a simple majority.

14 HISTORY OF COUNCIL RESOLUTION ESTABLISHING THE COMMITTEE

- 14.1 The Audit and Risk Committee was established by Resolution of the Shire of Dardanup Council on 23 October 2019.

15 OFFICER(S) RESPONSIBLE FOR MANAGEMENT OF THE COMMITTEE

- 15.1 The Chief Executive Officer shall appoint an officer relative to the Committee's Terms of Reference to manage the committee. In normal circumstances this is the Deputy Chief Executive Officer / Director Corporate & Governance.
- 15.2 The appointed officer shall provide the secretarial and administrative support through his/her Directorate.



**AUDIT & RISK COMMITTEE
CHARTER**

**INSTRUMENT OF APPOINTMENT
&
TERMS OF REFERENCE**

2020

By Resolution of Council
Ordinary Council Meeting [INSERT DATE HERE]
Resolution Number [XXX-20]



(Appendix AAR: 8.2C)

1 INTRODUCTION 1
2 ~~NAME~~ 1
3 CULTURE – AUDIT AND RISK..... 1
4 OBJECTIVES – GENERIC..... 1
5 FUNCTIONS OF THE AUDIT AND RISK COMMITTEE 2
6 COMMITTEE OBJECTIVES - SPECIFIC 2
7 MEMBERSHIP 3
8 PRESIDING MEMBER..... 5
9 MEETINGS..... 6
10 QUORUM..... 6
11 DELEGATED POWERS 6
12 TERMINATION OF COMMITTEE 7
13 AMENDMENT TO THE INSTRUMENT OF APPOINTMENT AND DELEGATION..... 7
14 COMMITTEE DECISIONS 7
15 HISTORY OF COUNCIL RESOLUTION ESTABLISHING THE COMMITTEE 7
16 OFFICER(S) RESPONSIBLE FOR MANAGEMENT OF THE COMMITTEE 8
17 ANNUAL CONFIRMATION OF RESPONSIBILITIES AND REVIEW OF ToR's 8
18 TRIENNIAL INDEPENDENT ASSESSMENT OF COMMITTEE PERFORMANCE 8
19 ANNUAL WORK PLAN 8
APPENDIX A 9

(Appendix AAR: 8.2C)

1 INTRODUCTION

- 1.1 The Council of the Shire of Dardanup (the "Council") establishes this committee under the powers given in Section 7.1A of the Local Government Act 1995, the committee to be known as the Audit and Risk Committee, (the "Committee").
- 1.2 The Council appoints to the Committee those persons to be members of the committee by resolution of Council. Membership of the Committee shall, unless otherwise specified, be for a term ceasing on the day prior to local government elections being held. Council may appoint members for a further term at the next available meeting following the elections.
- 1.3 The Committee shall act for and on behalf of Council in accordance with provisions of the Local Government Act 1995, local laws and the policies of the Shire of Dardanup and this instrument.
- 1.4 The Committee provides appropriate advice and recommendations to the Council on matters relevant to its Terms of Reference (ToR). This is in order to facilitate informed decision-making by the Council in relation to the legislative functions and duties of the local government that have not been delegated to the Chief Executive Officer ("CEO").

~~2~~ NAME

~~The name of the Committee is the "Audit and Risk" Committee.~~

3 CULTURE – AUDIT AND RISK

The Council of the Shire of Dardanup acknowledges that forward thinking accountable authorities and Audit and Risk Committees strive to maintain a sound culture within the entity to protect it from breakdowns in controls or fraud.

Even though the culture of an entity cannot be seen, it is a fundamental part of strong governance.

The Strategic Community Plan Leadership Objective 1 states: "Strong civic leadership representing the whole of the Shire which is supported by responsible and transparent corporate governance."

4 OBJECTIVES – GENERIC

The following objectives are generic to all Council committees:

- 4.1 To consider, advise and assist the local government in performing specified functions or fulfilling required responsibilities within its district;

(Appendix AAR: 8.2C)

- 4.2 Where appropriate, to liaise with relevant agencies and other persons in the development, review and testing of Council policy and strategic objectives;
- 4.3 To carry out research and other activities as directed by the Council or prescribed by the regulations; and
- 4.4 To fulfil the objectives and/or undertake the specific tasks as a Committee of Council specified in **Section 5** – Functions of the Committee and **Section 6** Committee Objectives - Specific.
- 4.5 To ensure that all members dealings are carried out in accordance with the Shire of Dardanup Code of Conduct.

(Details of tasks to be endorsed by Council by resolution when the committee is established or as amended from time to time).

5 FUNCTIONS OF THE AUDIT AND RISK COMMITTEE

The detailed functions of the Committee are set out in the Local Government (Audit) Regulations 1996, Regulation 14, 16 and 17.

6 COMMITTEE OBJECTIVES - SPECIFIC

The Audit and Risk Committee shall have the following objectives:

- 6.1 To meet with the auditor, once in each year and provide a report to Council on the matters⁷ discussed and outcome of those discussions;
- 6.2 **To meet with the auditor, at least once per year without management present (closed door session). The Committee will discuss matters relating to the conduct of the audit, including any difficulties encountered, restrictions on scope of activities or access to information, significant disagreements with management and adequacy of management responses;**
- 6.3 Provide an effective means of communication between the external and internal auditors;
- 6.4 Examine the reports of the auditor to –
 - i.) determine if any matters raised require action to be taken by the local government; and
 - ii.) ensure that appropriate action is taken in respect of those matters;
- 6.5 Review annually the internal audit plan, including any reports produced as part of special assignments undertaken by internal audit.
- 6.6 To consider the Financial Management Systems Review required every three years under Regulation 5 of the *Local Government (Financial Management) Regulations 1996*, and report to Council the results of that review;

(Appendix AAR: 8.2C)

- 6.7 Consider and recommend adoption of the Annual Financial Report to Council.
- 6.8 To consider the Shire of Dardanup Risk Management Governance Framework (once in every 3 years) for appropriateness and effectiveness and progress on the relevant action plans biannually.
- 6.9 To consider the CEO's triennial reviews of the appropriateness and effectiveness of the Shire's systems and procedures in regard to risk management, internal control and legislative compliance, required to be provided to the Committee, and report to the Council the results of those reviews – Local Government (Audit) Regulations 1996 Regulation 17.
- 6.10 Legislative Compliance - Oversee the effectiveness of the systems for monitoring compliance with relevant laws, regulations and associated government policies. This includes:
- i.) review the annual Compliance Audit Return (CAR) in accordance with section 7.13(1)(i) of the Local Government Act and report to the Council the results of that review; and
 - ii.) receive the biannual compliance report resulting from the Compliance Manual (incorporating the annual calendar).
- 6.11 To consider the CEO's biennial Governance Health and Financial Sustainability review and report to the Council the results of that review.
- 6.12 To consider that relevant mechanisms are in place to review and implement, where appropriate, issues raised in OAG better practice guides and performance audits of other State and local government entities.
- 6.13 To consider the Information Systems Security biennial review, and report to the Council the results of that review.

Any variation to these objectives is not to be considered by the Committee unless approved by Council.

7 MEMBERSHIP

- 7.1 The Council resolves to nominate no more than five elected members as members for the Committee for a period of two years or until the next Ordinary Council election, the five elected members shall be members of the committee.

[Note: It is recommended that at least half of the committee members are made up of elected members that are commencing their 4 year term; with the other half being elected members that are midway through their term on Council.]

(Appendix AAR: 8.2C)

- 7.2 The members, taken collectively, will have a broad range of skills and experience relevant to the operations of the Council. At least one (1) member of the Committee should have accounting or related financial and/or risk management experience.
- 7.3 Where the desirable accounting or related financial and/or risk management experience cannot be attained from the elected members, membership to the Committee may be extended to one (1) independent external member.
- 7.4 Independent external members (if required) will be selected based on the following criteria:
 - 7.4.1 A suitably qualified person with demonstrated high level of expertise and knowledge in financial management, risk management, governance and audit (internal and external);
 - 7.4.2 Understanding of the duties and responsibilities of the position; ideally with respect to local government financial reporting and auditing requirements;
 - 7.4.3 Strong communication skills; and
 - 7.4.4 Relevant skills and experience in providing independent expert advice.
- 7.5 An independent external member will be a person with no operating responsibilities with the Council nor will that person provide paid services to the Council either directly or indirectly.
- 7.6 Appointment and re-appointment of independent external members shall be made by Council after consideration of the CEO's recommendation. The applications of independent external members will be sought through an open and transparent Expression of Interest process. The evaluation of potential members will be reviewed by the CEO and Deputy CEO, with appointments to be approved by the Audit & Risk Committee and Council. Appointments will be for a maximum term of two (2) years and align with the biennial Council election cycle. Independent external members will not be appointed for more than three (3) consecutive terms.
- 7.7 Independent external members will be required to complete a confidentiality agreement and confirm that they will operate in accordance with the Council's Code of Conduct.
- 7.8 The Council may by resolution terminate the appointment of any independent external member prior to the expiry of his/her term if:
 - 7.8.1 The Committee by majority determines that the member is not making a positive contribution to the Committee; or
 - 7.8.2 The member is found to be in breach of the Council's Code of Conduct or a serious contravention of the Local Government Act 1995;
or

(Appendix AAR: 8.2C)

- 7.8.3 A member's conduct, action or comments brings the Council into disrepute.
- 7.9 Reimbursement of approved expenses may be paid to the independent external member in accordance with the Local Government Act Section 5.100.
- 7.10 New members will receive relevant information and briefings on their appointment to assist them to meet their Committee responsibilities. The Deputy Chief Executive Officer will undertake a formal induction process for new members to the Committee at the first Committee meeting post-election.
- 7.11 Membership is prescribed by the Local Government Act 1995 Section 7.1A.
- 7.12 Specific membership of the Audit and Risk Committee are outlined in sections 5.10 and 5.11 of the *Local Government Act 1995*.

8 PRESIDING MEMBER

- 8.1 The CEO or delegated nominee will preside until the position of Presiding member is filled in accordance with Schedule 2.3 clause 3 of the *Local Government Act 1995*.
- 8.2 The Committee shall appoint a Presiding Member and Deputy Presiding Member to conduct its business in accordance with the following provisions of Section 5.12 of the *Local Government Act 1995*.
- 8.3 The Presiding Member shall ensure that business is conducted in accordance with the Shire of Dardanup Standing Orders and that minutes of the proceedings are kept in accordance with Section 5.22 of the *Local Government Act 1995*.
- 8.4 The Deputy presiding member has the following functions as per section 5.13 of the *Local Government Act 1995*.
- 8.5 A presiding member is to be chosen from the committee members present at the meeting if the presiding member or deputy presiding member are unavailable or unwilling to perform the functions of the presiding member in accordance with Section 5.14 the *Local Government Act 1995*.
- 8.6 The presiding member plays an important role in leading and guiding discussions at committee meetings. The presiding member shall have the right interpersonal skills to guide discussions on complex and sensitive matters.
- 8.7 To maintain independence and a Committee that is free of undue or improper influence, the presiding member shall not be the Shire President. The Shire President will Chair the Ordinary Council Meetings where the Committee meeting minutes will be confirmed.

(Appendix AAR: 8.2C)

9 MEETINGS

~~9.1 As there are no power or duty delegated to the committee the meetings are not open to the public.~~

9.1 In accordance with Section 5.23 of the Local Government Act 1995 the meetings will be generally open to the public as the Committee has a power or duty that has been delegated by Council (refer part 11).

9.2 The Committee shall meet on a quarterly basis, with a minimum of **4 meetings** per year, dates to be resolved by the Committee but generally March, June, September and December.

9.3 Notice of meetings including an agenda shall be given to members at least **5 days** prior to each meeting.

9.4 The Presiding member shall ensure that detailed minutes of all meetings are kept and shall, not later than **5 days** after each meeting, provide the members and Council with a copy of such minutes.

9.5 The minutes of the meeting are to be included in the next available Ordinary meeting of Council agenda for consideration of recommendations or to be received by the Council.

9.6 All members of the Committee shall have one vote. If the vote of the members present are equally divided, the person presiding is to cast a second vote.

9.7 Shire of Dardanup Local Law Standing Orders apply to all Shire of Dardanup committees.

10 QUORUM

10.1 Quorum for a meeting shall be at least 50% of the number of offices, whether vacant or not. A decision of the Committee does not have effect unless it has been made by a simple majority.

[Note: Council may, at the request of the Committee, agree to set the quorum at a lesser number. However in such circumstances any recommendation on expenditure of monies or on forming policy positions that is being made to Council or the CEO, the committee must have at least 50% of the members present to make a valid recommendation/s.]

11 DELEGATED POWERS

~~11.1 The Committee has no specific powers under the Local Government Act and is to advise and make recommendations to Council only.~~ Pursuant to section

(Appendix AAR: 8.2C)

5.17 of the Act, the Committee is delegated the power to conduct the formal meeting with the Auditor required by Section 7.12(A)(2) on behalf of the local government.

11.2 In all other matters, Committee recommendations shall not be binding on Council and must be endorsed by Council to take effect.

11.3 The Council reserves the right to delegate powers to the committee if circumstances require delegation. The Delegation shall be recorded in the Council minutes prior to the delegation being exercised.

12 TERMINATION OF COMMITTEE

Termination of the Committee shall be:

12.1 In accordance with the Local Government Act 1995; or

12.2 At the direction of Council; or

12.3 On the specified date.

13 AMENDMENT TO THE INSTRUMENT OF APPOINTMENT AND DELEGATION

13.1 This document may be altered at any time by the Council on the recommendation of the Committee, or by direct resolution of Council.

14 COMMITTEE DECISIONS

~~14.1 Committee decisions shall not be binding on Council in any circumstance.~~

Cindy note: refer ToR 11 and delegation 1.1.1 which gives the committee:

~~3. Authority to review and **endorse** the Shire of Dardanup's report on any actions taken in response to an Auditor's report, prior to it being forwarded to the Minister within 3 months after the audit report is received by the Shire of Dardanup. [s.7.12A(4)].~~

14.2 The decisions of the Audit and Risk Committee is to be by simple majority in accordance with Section 7.1C of the *Local Government Act 1995*.

15 HISTORY OF COUNCIL RESOLUTION ESTABLISHING THE COMMITTEE

15.1 The Audit and Risk Committee was established by Resolution of the Shire of Dardanup Council on 23 October 2019.

(Appendix AAR: 8.2C)

16 OFFICER(S) RESPONSIBLE FOR MANAGEMENT OF THE COMMITTEE

- 16.1 The Chief Executive Officer shall appoint an officer relative to the Committee's Terms of Reference to manage the committee. In normal circumstances this is the Deputy Chief Executive Officer / Director Corporate & Governance.
- 16.2 The appointed officer shall provide the secretarial and administrative support through his/her Directorate.

17 CONFIRMATION OF RESPONSIBILITIES AND REVIEW OF ToR's

- 17.1 The Committee will confirm annually that all responsibilities outlined in this ToR have been carried out. The annual confirmation will be reported through to Council and will include information about the Committee and the outcomes delivered during the period.
- 17.2 Every two (2) years the Terms of Reference shall be reviewed by the Committee.

18 BIENNIAL INDEPENDENT ASSESSMENT OF COMMITTEE PERFORMANCE

- 18.1 An independent external assessment of the Committee is undertaken at least once in every two (2) years. This assessment may be included in the scope of audit for the Governance Health and Financial Sustainability Review.

19 ANNUAL WORK PLAN

- 19.1 A forward annual work plan will be agreed by the Committee each year. The forward annual work plan will cover all Committee responsibilities as detailed in this ToR.
- 19.2 An example of the Annual Work Plan is provided in Appendix A.

APPENDIX A

AUDIT AND RISK COMMITTEE – XXXX ANNUAL WORK PLAN				
FUNCTIONS, RESPONSIBILITIES & ASSOCIATED ACTIVITIES	XX XX	XX XX	XX XX	XX XX
1. Committee Operation				
Biennial review of the Charter (Terms of Reference)				
Agree on the annual work plan; and set priority areas for the coming year				
Recruitment of an external member to the committee (if required)				
Annual confirmation that all responsibilities outlined in the Charter have been carried out. The annual confirmation will be reported through to Council and will include information about the Committee and the outcomes delivered during the period				
New members are briefed on their appointment to assist them to meet their Committee responsibilities.				
Appointment of Presiding Member and Deputy Presiding Member				
2. Risk Management				
To consider the Risk Management Governance Framework (once in every 3 years) for appropriateness and effectiveness (report next Due: XX-XX-XXXX)				
Receive the biannual dashboard report				
3. Legislative Compliance				
Review the annual Compliance Audit Return (CAR) and report to the Council the results of that review				
Receive the biannual compliance report resulting from the Compliance Manual (incorporating the annual calendar)				
4. Internal Audit				
Review annually the internal audit annual work plan, including any reports produced as part of special assignments undertaken by internal audit				
5. Financial Reporting				
Consider and recommend adoption of the Annual Financial Report to Council				
6. External Audit (OAG)				
To meet with the auditor, once in each year and provide a report to Council on the matters discussed and outcome of those discussions				

(Appendix AAR: 8.2C)

AUDIT AND RISK COMMITTEE – XXXX ANNUAL WORK PLAN				
FUNCTIONS, RESPONSIBILITIES & ASSOCIATED ACTIVITIES	XX XX	XX XX	XX XX	XX XX
To meet with the auditor, at least once per year without management present (closed door session). The Committee will discuss matters relating to the conduct of the audit, including any difficulties encountered, restrictions on scope of activities or access to information, significant disagreements with management and adequacy of management responses				
Examine the reports of the auditor to – i.) determine if any matters raised require action to be taken by the local government; and ii.) ensure that appropriate action is taken in respect of those matters				
To consider that relevant mechanisms are in place to review and implement, where appropriate, issues raised in OAG better practice guides and performance audits of other State and local government entities.				
7. Regulation 17 Triennial Review (report next Due: XX-XX-XXXX)				
To consider the CEO's triennial review on risk management, internal control and legislative compliance				
Set the action plan arising from auditor recommendations from the Regulation 17 review				
Receive an update on the action plan arising from auditor recommendations from the Regulation 17 review				
8. Financial Management Systems Triennial Review (report next Due: XX-XX-XXXX)				
To consider the Financial Management Systems Review required every three years under Regulation 5 of the Local Government (Financial Management) Regulations 1996, and report to Council the results of that review				
Set the action plan arising from auditor recommendations from the Financial Management Systems Review				
Receive an update on the action plan arising from auditor recommendations from the Financial Management Systems Review				
9. Governance Health and Financial Sustainability Biennial Review (report next Due: XX-XX-XXXX)				
To consider the CEO's biennial Governance Health and Financial Sustainability Review, and				

(Appendix AAR: 8.2C)

AUDIT AND RISK COMMITTEE – XXXX ANNUAL WORK PLAN				
FUNCTIONS, RESPONSIBILITIES & ASSOCIATED ACTIVITIES	XX XX	XX XX	XX XX	XX XX
report to the Council the results of that review				
Set the action plan arising from auditor recommendations from the Governance Health and Financial Sustainability Review				
Receive an update on the action plan arising from auditor recommendations from the Governance Health and Financial Sustainability Review				
Undertake an independent external assessment of the Committee at least once in every three years. This assessment may be included in the scope of audit for the Governance Health and Financial Sustainability Review				
10. Information Systems Security Audit (report next Due: XX-XX-XXXX)				
Receive the audit report arising from the 2 yearly Information Systems Security Audit				
Set the action plan arising from the recommendations from the Information Systems Security Audit				
Receive an update on the action plan arising from the recommendations from the Information Systems Security Audit				

RISK ASSESSMENT TOOL**OVERALL RISK EVENT:** 2020 Compliance Calendar – Bi-annual 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.




1 Council Drive
EATON WA 6232

INTERNAL AUDIT STRATEGIC PLAN

2020/21 – 2022/23



(Appendix AAR: 8.4A)

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	14-08-2019
2.0	23/06/2020	Annual update of plan	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	

Contents

INTRODUCTION	1
INTERNAL AUDIT ACTIVITIES OVERVIEW	1
METHODOLOGY	3
INTERNAL AUDIT COVERAGE PRIORITISATION	4
OBJECTIVE	4
RESPONSIBILITIES	5
AUDITOR GENERAL REPORTS	5
INTERNAL AUDIT ANNUAL WORK PLAN	6
ANNUAL AUDIT REVIEW 2020 - 2021	7
TEMPLATE – INTERNAL AUDIT ASSESSMENT AND RESPONSE SUMMARY	8

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 line with the presentation of the annual financial report audit to the Audit and Risk Committee.

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;

(Appendix AAR: 8.4A)

- 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; and
- 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 party;
 - 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.

(Appendix AAR: 8.4A)

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 Compliance 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 governments 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 audit function under Regulation 17.

(Appendix AAR: 8.4A)

INTERNAL AUDIT ANNUAL WORK PLAN

INTERNAL AUDIT ANNUAL WORK SCHEDULE 2020 - 2021					
PROJECT	TYPE	RISK RATING	BUDGET DAYS	DATE	RESOURCES
Procurement	Assurance – Performance (Improvement) Review	Moderate - High	6 months	August 2020 to February 2021	Compliance Officer
Receipting Petty Cash	Assurance - Financial; Compliance	Low	5	March 2021	Compliance Officer
Rating Rates Levied	Assurance - Financial; Compliance	Moderate	12	April 2021	Compliance Officer
Payables Creditors	Assurance - Financial; Compliance	Moderate	10	May 2021	Compliance Officer
Law Enforcement ZooData Ranger Infringements	Assurance - Financial; Compliance	Moderate	7	June 2021	Compliance Officer

ANNUAL AUDIT REVIEW 2020 - 2021

The 2020-2021 Internal Audit Plan will conduct an audit review of 5 areas of the Shire of Dardanup operations:

Procurement

Performance (Improvement) Review

- Tender Scheduling
- Preferred Supplier Panel
- Templates and Forms
- Procurement Toolkit (Intranet)

Receipting – Petty Cash

Internal Controls
Transaction Verification
Authorising Process
Processing
Compliance
Payments

Rating – Rates Levied

Internal Controls
Transaction Verification
Authorising Process
Processing
Compliance

Payables – Creditors

Internal Controls
Transaction Verification
Authorising Process
Processing
Compliance
Payments

Law Enforcement – ZooData Ranger

Infringements

Internal Controls
Transaction Verification
Authorising Process
Processing
Compliance
Payments

All audit assessment areas above will initially have 4 tests, this testing may be extended if areas of concern are noted.

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: 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.	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 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.	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.	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.



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
Fax: 08 6557 7600
Email: info@audit.wa.gov.au

Dear Mr Schonfeldt

**ANNUAL FINANCIAL REPORT
INTERIM AUDIT RESULTS FOR THE YEAR ENDED 30 JUNE 2020**

We have completed the interim audit for the year ended 30 June 2020. 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.

Management Control Issues

I would like to draw your attention to the attached listing of deficiencies in internal control and other matters that were identified during the course of the interim audit. These matters have been discussed with management and their comments have been included on the attachment. The matters reported are limited to those deficiencies that were identified during the interim audit that we have concluded are of sufficient importance to merit being reported to management. Some of the matters may be included in our auditor's report in accordance with section 7.9(2) of the *Local Government Act 1995* or regulation 10(3)(a) and (b) of the *Local Government (Audit) Regulations 1996*. If so, we will inform you before we finalise the report.

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 CA
ASSISTANT DIRECTOR
FINANCIAL AUDIT
21 August 2020

Attach

SHIRE OF DARDANUP

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2020

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

INDEX OF FINDINGS	RATING		
	Significant	Moderate	Minor
1. Verbal Quotations not Documented		✓	

KEY TO RATINGS

The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

- Significant** - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly.
- Moderate** - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.
- Minor** - Those findings that are not of primary concern but still warrant action being taken.

SHIRE OF DARDANUP

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2020

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

1. Verbal Quotations not Documented

Finding:

During our procurement testing, we noted 6 purchases below \$2,999, out of a sample of 60, where verbal quotes was not documented in the purchase orders to confirm that verbal quotes had been obtained.

The Shire’s procurement policy states that where the value of a purchase is below \$2,999 and where no Panel of Pre-Qualified Suppliers exist at least one verbal or written quote must be obtained. The procurement procedure then provides further instruction stating that written notes detailing each verbal quotation must be recorded in the pre-printed verbal quotation section of the Office Copy Purchase Order.

Rating: Moderate

Implication:

If the information is not captured in accordance with the Shire’s procurement procedure, it would be difficult for management to ascertain if verbal quotes were obtained.

Recommendation:

We recommend that verbal quotations are documented on the purchase order in accordance with the procurement procedure to evidence that the verbal quotation were obtained.

Management’s Comments:

It is agreed that during the 2019/20 Interim Audit that six (6) samples of Purchase Orders did not explicitly contain or document the Verbal Quotations on the Office Copy of the Purchase Order. Whilst Council can confirm that each Authorising Officer did receive a Verbal Quotation at the time the goods and/or services were procured, failure to record the Verbal Quotation on the Purchase Order has resulted in non-compliance to Councils internal procedure document PR045 – Procurement Procedure.

Management is of the view that the Verbal Quotation requirements have been satisfied in accordance with Council’s adopted CP034 - Procurement Policy CP034, which requires one verbal or written quotation for goods and/or services purchased less than \$2,999. This was evident on each Purchase Order as the Verbal Quotation box was checked and ticked by the Authorising Officer.

Management acknowledge the non-compliance issue relating to Council’s internal documented procedure PR045 - Procurement Procedure which stipulates that ‘written notes detailing each verbal quotation must be recorded in the pre-printed verbal quotation section on the Office Copy Purchase Order’. Each Officer had ticked the ‘Verbal Quotation’ box received – but not recorded the Verbal Quotation in the section provided on the Purchase Order.

The following purchases pertain to the Finding ‘Verbal Quotations not documented’.

Item	Supplier	Purchase Description	Value
1.	Go Electrical Contracting	Repairs to ERC Carpark Lighting	\$110.00
2.	Keith Williams & Co	Replace Ute Tarp	\$60.50
3.	South West Locksmiths	Rekey Internal Office Door Entry at ERC	\$137.65
4.	Quality Press	Vehicle ID stickers for Brigades	\$70.99
5.	Total Hygiene	ERC Sanitary Service	\$1,485.00
6.	Bunbury Subaru	Vehicle Service	\$401.42

SHIRE OF DARDANUP

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2020

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

In addressing this non-compliance issue relating to Council's procurement procedures, Management communicated with each Authorising Officer responsible to remind them of the obligation to record and document the Verbal Quotations on the physical purchase order. In response, all Authorising Officers' advised that:

- Verbal Quotations were sought.
- the Verbal Quotations box had been ticked; however,
- due to an error or lapse in judgement – the verbal quotations were not documented (written) on the Purchase Order which has resulted in the non-compliance of Procurement Procedure PR045.

Additionally Council's Procurement Officer has increased the scope for in-house Procurement Training for Requisition and Authorising Officers' including a 'refresher' training workshop that is scheduled to be rolled out across the organisation.

In summary Management agrees with the audit recommendation that Verbal Quotations should be recorded on the Purchase Order in accordance with Council's Procurement Procedure. However, Council is of the view the Finding should be classified as 'Minor' - as *opposed to 'Moderate'* - due to each Purchase Order:

- indicating Verbal Quotations were sought (through the tick box actioned);
 - in our opinion - compliant to the adopted Council Policy CP034;
 - compliant to all other areas of the Procurement Procedure PR045 (excluding the written requirement of Verbal Quotations); and
 - with the Finding in the lowest threshold purchasing bracket of Goods and Services 'Less than \$2,999';
- Management are of the view the Finding 'Verbal Quotations not documented' should be considered 'Minor'.

Responsible Person: Deputy Chief Executive Officer
Completion Date: 17 August 2020

RISK ASSESSMENT TOOL									
Annual Financial Report – Interim Audit Results for the Year Ending 30 June 2020									
RISK THEME PROFILE:									
3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory) 12 - Misconduct									
8 - Errors, Omissions and Delays									
RISK ASSESSMENT CONTEXT: Operational									
CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER 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 presenting the Interim Audit Results for the year ending 30 June 2020 to the Audit and Risk Committee (and subsequently Council).	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 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.	
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.	

