Western Australian
Auditor General's Report

Fraud Prevention in Local Government

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Gareth Govan
Adam Dias

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.

ISSN: 2200-1931 (Print)
ISSN: 2200-1921 (Online)

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Fraud Prevention in Local Government

Report 5
August 2019

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

FRAUD PREVENTION IN LOCAL GOVERNMENT

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 200*6.

This was a narrow scope performance audit, conducted under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target entity compliance with legislation, public sector policies and accepted good practice.

The audit objective was to assess whether local government entities have taken appropriate steps to prevent fraud.

I wish to acknowledge the cooperation of staff at the local government entities included in this audit.

CAROLINE SPENCER
AUDITOR GENERAL
15 August 2019

Contents

Auditor General's overview

All organisations, public and private, face the risk of fraud. This will remain the case wherever people and scarce resources interact. Fraud, or even the perception of fraud, can have a serious impact on an organisation's reputation and resources. It can stem from inside or outside the organisation and by its nature is deceitful, dishonest, and often hard to detect. Numerous Corruption and Crime Commission investigations highlight the risks organisations face.

However, there are practical steps organisations can take to reduce fraud risks and build their fraud resistance. These include creation of a strong ethical culture that sets the standard of behaviour for all staff, raising staff awareness of the risks, and implementing good practice controls to manage them.

This audit found that many local governments have not assessed their fraud risks, and do not have comprehensive fraud management plans and programs. Most could do more to educate their staff on integrity polices and controls to reinforce anti-fraud messages and consider fraud risks in their daily duties. Local governments also need to make sure they have clear and easy processes for people to report any fraud concerns.

It was pleasing to find that all the local governments we reviewed had some fraud controls in place and the staff my audit team dealt with during the audit were diligent. But, high staff turnover and work load makes implementing good fraud controls even more of a priority.

I would like to acknowledge the willingness of the entire sector to engage with our questionnaire. Nearly 80% of local governments responded, providing valuable information about fraud approaches across the local government sector.

I encourage all entities to use the principles highlighted in Appendix 2 to build on their existing structures and practices, in a way that best suits their needs.

Executive summary

Introduction

Recent high profile investigations into fraud in the public sector by the Corruption and Crime Commission (CCC) in Western Australia (WA) have featured a number of local government entities (entities).

There are 148 entities in WA. In 2017-18, the sector spent more than $4 billion, employed around 17,000 staff, and administered $45 billion of assets. Fraud in this sector could result in substantial material and reputational losses, and this level of risk calls for entities to implement strong controls and better practice approaches to reduce the threat of fraud.

This audit reviewed whether entities have taken appropriate steps to prevent fraud, through the following lines of inquiry:

1. Have entities implemented a coordinated approach to manage fraud risks?
2. Do entities have adequate controls for preventing and detecting fraud?
3. Do entities respond appropriately to suspected fraud?

The purpose of this audit was to review the systems that entities had in place. We did not seek to identify any specific instances of fraud.

The audit included a sector wide questionnaire on entity approaches to managing fraud risks (see Appendix 3 for a summary of results). We conducted a more detailed review at the:

- Shire of East Pilbara
- Shire of Katanning
- City of Nedlands
- Shire of Serpentine-Jarrahdale
- City of Vincent.

Our sample focussed on entities that had not been part of recent audits, and included entities of varying size, from both metropolitan and regional areas.

Conclusion

Local government entities can do more to prevent fraud. We found entities do have some controls in place, but would benefit from better understanding their specific fraud risks and taking a coordinated approach to managing them.

Our questionnaire found many entities have not assessed their fraud risks, or created a plan to deal with fraud. The responses highlighted gaps in prevention and detection approaches. Many entities can do more to raise staff awareness of fraud, improve their screening processes, and strengthen protections for informants.

Our detailed review of 5 entities confirmed these results. We found they had core integrity policies in place, but none had assessed all their fraud risks, and implemented a coordinated approach to manage them. All entities could build on their current policies and practices to make workplaces more fraud resistant, and improve their reporting avenues to strengthen their ability to respond to fraud.

Background

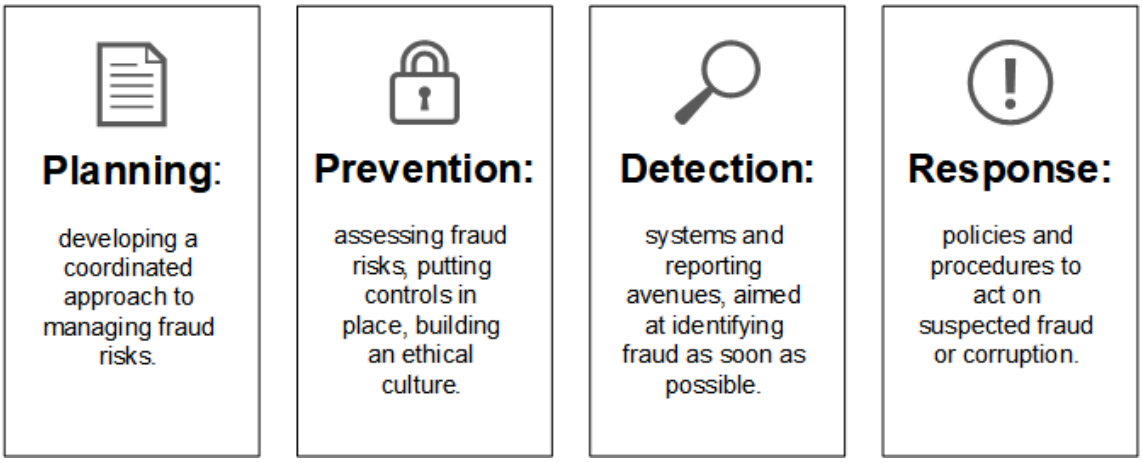
Fraud is the act of obtaining a benefit, financial or otherwise, by deception. By its nature it is deceitful and dishonest, and can be very hard to detect particularly if collusion is involved. It is important that public sector entities design and implement strong internal control frameworks to prevent fraud.

Meeting legislated requirements provides entities with some level of fraud control (Appendix 1), particularly around council decision-making processes. Legislation includes requirements for:

- council and advisors to disclose conflicts of interest
- disclosure of financial interests for some staff
- the creation of Codes of Conduct
- handling of gifts
- when tendering is required for procurement activities.

This is the second report that we have tabled on public sector fraud controls. The previous report in 2013 reviewed 9 state government entities against elements taken from the *Australian Standard AS 8001-2008 Fraud and Corruption Control* (the Standard).

The Standard contains better practice guidance for controlling fraud risks. It is informative, flexible, and forms the basis of approaches in state and local government entities across Australia. It recommends entities tailor an approach that suits their needs, based on 4 components:



In developing our expectations for entities, we considered:

- key principles from the Standard
- guidance issued to entities by the Department of Local Government, Sport and Cultural Industries
- reports published by the CCC and the Public Sector Commission (PSC)
- guidance material issued by audit offices in other jurisdictions
- the best practice guide for fraud and corruption control published by the Crime and Corruption Commission in Queensland
- international research.

Recommendations

In line with better practice, all entities should ensure they implement a coordinated approach to manage their fraud risks. Entities should:

1. assess fraud risks across their business
2. develop a Fraud and Corruption Control Plan and review it at least once every 2 years
3. develop and implement a periodic fraud awareness training program for all staff
4. ensure that all conflicts of interest are recorded, assessed and appropriate management plans are in place
5. have policies and procedures in place to verify the identity and integrity of employees and suppliers
6. document clear internal processes and systems to report any potential fraud, that include anonymous reporting
7. collect and analyse information received about potential fraud to identify any trends or emerging issues.

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 audited local government entities

All 5 audited entities supported the audit findings and accepted our recommendations. Appendix 4 includes the full responses from audited entities.

Audit findings

Entities have not implemented a coordinated approach to manage their fraud risks

We found that entities have not developed a good understanding of their fraud risks, or a clear vision of how they will manage them. As a result, entities cannot be sure they have adequate controls in place. These findings are similar to those of our 2013 audit into State government entity fraud controls, which found a lack of risk assessment and planning[1].

Entities have not assessed their business for fraud risks

None of the entities we reviewed had assessed all their fraud risks. We found strategic risk registers included some consideration of external theft and fraud. But, these were incomplete, focussed on external threats, and did not consider all fraud risks. This supports results from our questionnaire, as 25% of respondents told us they had not completed a fraud risk assessment. Completing an assessment would give entities a view of all their risks, and allow them to evaluate their controls.

Twenty-nine of the 116 entities (25%) that responded to this part of our questionnaire advised that they had not assessed their fraud risks. These entities had a combined expenditure of over $310 million in 2017-18.

Entities have not planned how to manage fraud risks

We found that most entities have not developed a Fraud and Corruption Control Plan (Plan). These results are similar to those from our 2013 audit of fraud prevention in State government entities[2]. That audit reviewed 9 State government entities and found none had developed a Plan. Plans are important better practice tools that capture an entity's commitment to manage its fraud risks, communicate its approach, and set timeframes and responsibilities.

Of the entities reviewed, only East Pilbara had developed a Plan. While the Shire completed this in 2013, it has not implemented any of the Plan's actions.

All 5 entities had Codes of Conduct (Codes) and East Pilbara, Nedlands and Vincent also have strategic fraud prevention policies. While these contain anti-fraud information, they are not as comprehensive as a Plan as they do not include controls, or assign timeframes or responsibilities for actions. Without a Plan, entities cannot be sure their approach to managing fraud risks is comprehensive.

Responses to the questionnaire show this is an issue across the sector, as more than half (54%) the entities told us they had not created a Plan.

We received documents from 26 of the entities who told us they had a Plan or equivalent. However, we found only 7 of these contained all the key elements of the Standard[3]. A further 8 contained at least 2 of the elements. Avenues for reporting suspected fraud, key controls to deal with fraud related risks and comprehensive fraud risk assessments were elements that were most commonly absent.

[1] Office of the Auditor General 2013 *Fraud prevention and detection in the Public Sector*. Report 7 – June.

[2] Ibid.

[3] We reviewed the documents for key elements of the Standard including an entity position statement, accountabilities, a fraud risk assessment, outline of key controls, and reporting avenues and protections.

Entities could make themselves more fraud resistant if they strengthen their controls

We found that entities could make their organisations more fraud resistant if they raise staff awareness of risks, improve how they manage conflicts of interests, and better screen employees and suppliers.

Entities need to raise staff awareness of fraud risks

The Standard describes building a strong anti-fraud culture as a key strategy for managing the risk of fraud. Messaging to staff can help entities build and maintain fraud resistant cultures. Entities should commit to a program to raise staff awareness of integrity policies. By tracking participation they can be sure staff are aware of risks, the controls that are in place, and their responsibilities.

We found entities have not established regular programs to raise and maintain staff awareness of fraud risks. None of the entities we reviewed had established a regular training program, or had kept records of staff participation. The questionnaire provided similar results, with 55% of entities advising they did not train staff in fraud risks and controls.

Some of the entities we reviewed have made efforts to raise staff awareness of fraud risks and integrity policies. We found:

- 3 entities had used training, forums, or newsletters to engage staff in managing fraud risks (Figure1)
- 2 entities had tailored the language in their Codes to make them easier for staff to understand. To explain conflicts of interest, Serpentine-Jarrahdale used plain English rather than text from legislation, and Katanning included “real world” examples.

Katanning	Nedlands	Serpentine-Jarrahdale
The Infrastructure Department received refresher training on the Shire’s code of conduct in January 2019.	Information about integrity issues have been included in staff newsletters. For example: • information on ethical decision making – August 2018 • article on conflicts of interest - September 2018.	The Shire has conducted a series of staff forums. For example: • CEO led a forum on fraud controls - March and April 2017 • ‘good governance’ forum - September 2018 • forum on misconduct prevention, including a presentation from the PSC - January 2019.

Source: OAG using entity information

Figure 1. Examples of recent efforts to raise fraud awareness

All the entities we reviewed provided employees with key integrity policies at induction. However, none required staff to revisit the policies. The Standard recommends all employees confirm they understand and follow the Code, and other integrity policies, on a yearly basis. Results from our questionnaire suggest this is an issue across the sector, as 89% of entities told us they do not require staff to do this. Recording annual compliance would give entities a level of assurance that staff are regularly engaging with integrity policies and messages.

Not all conflicts of interest are captured

Three of the entities we reviewed did not capture all the conflicts of interest their staff may face. In line with legislation, entities record conflicts of staff and elected members on matters discussed by council. Entities also document financial, proximity and impartiality interests of elected members and senior staff.

However, processes are not in place to capture, assess and manage any other interests staff have that may conflict with their daily duties. Entities cannot be sure they appropriately manage all conflicts of interest (actual, potential or perceived), as they rely on individual business units to handle operational issues with no formal guidance or process. Staff need to be aware that they have a responsibility to declare any interests that could conflict with performing their public duties. Entities then need to capture and manage those declarations.

Vincent and Serpentine-Jarrahdale have recently implemented processes to better capture all conflicts of interest. Both entities have developed registers to capture the conflict, and require a manager or executive to approve the management plan. During the audit, both entities provided staff with guidance on how and when to make a declaration.

More screening of employees and suppliers would help entities reduce risks

The entities we reviewed did not have adequate policies to screen staff or suppliers. Good screening controls would give entities some assurance of the identity, integrity and credentials of employees and suppliers.

None of the entities we reviewed had policies in place to screen staff. These findings are similar to those in our 2019 audit *Verifying Employee Identities and Credentials*[4].

Despite the lack of policy, 4 entities did retain copies of qualifications and identification. However, none consistently confirmed that qualifications were authentic or checked work histories. One entity did not engage in any police checks or do any checks beyond calling referees. Entities need consistently applied processes to confirm the identity, integrity and academic credentials of potential employees. The Standard also recommends entities screen all new employees and any employee transferring to an executive or high-risk area.

None of the entities we reviewed routinely screened their suppliers. Our questionnaire returned similar results, with less than 30% of respondents conducting media searches, police clearances or verifying directors' details. Purchases over $150,000 are subject to tender which include some checks, including an ABN confirmation and receiving information on the financial position of the supplier. However, smaller purchases are not subject to this process.

To reduce fraud risks, the Standard recommends that entities verify the credentials of suppliers. Entities that have a large number of suppliers should consider a risk-based approach to screening to ensure appropriate use of resources.

Better reporting avenues would help entities detect and respond to fraud

To be well informed, entities need to have strong systems to receive, capture and act on information about potential fraud. International research has shown that organisations most frequently detect fraud through informants (whistleblowers)[5].

[4] Our audit found only 3 of the 8 entities reviewed had policies to verify employee identities and credentials.

[5] Association of Certified Fraud Examiners 2018 *Report to the nations: global study on occupational fraud and abuse*. p4.

We found that it was not always clear how staff, the public or suppliers should report suspected fraud. The entities we reviewed did not have ways for individuals to make anonymous reports of potential fraud, other than Public Interest Disclosures (PID) through the *Public Interest Disclosure Act 2003* (PID Act). They also did not have a process in place to analyse all information they received about potential fraud. Entities may miss important information if reporting avenues are not clear or if reports are not analysed.

Entities need to better communicate how staff, suppliers and the public can report suspicious behaviour

At the entities we reviewed, Codes direct staff to report concerns of fraud to the CEO, deputy, or HR manager. However, there is no guidance for how a staff member would do this. Staff members may be reluctant to go directly to the executive on such a sensitive topic or when the suspicion relates to senior staff. The Standard highlights the need for formalised reporting systems and that these should include multiple avenues. Similarly, the Crime and Corruption Commission in Queensland has advised that employees will feel more confident in making reports if systems are readily accessible and well publicised[6].

The PID Act encourages people to report concerns of wrongdoing in the public sector. Individuals can report concerns to authorised officers or to 1 of the authorities listed in the PID Act (such as the Auditor General for concerns including substantial unauthorised use of public resources). Other external reporting avenues include the CCC, PSC or the Western Australia Police Force.

All the entities we reviewed had clear processes around making a PID and had PID officers in place. However, entities should not rely only on PIDs, as this does not capture all potential reports or allegations. Staff may not wish to engage with the PID process or may not have information suitable for an investigation. The PSC reported that local government entities received 13 PIDs in 2017-18[7].

Our questionnaire showed that many other entities could improve their reporting processes and protections. One third of respondents told us they did not have systems in place to protect staff who reported fraud. Of those that did have protections, 32% told us they relied solely on PIDs. Individuals may be reluctant to report concerns if they do not feel adequately protected.

Entities should include anonymous reporting options to encourage reporting

At the entities we reviewed, internal avenues to report suspected fraud did not include anonymous options. Both the Standard and guidance from other jurisdictions has raised the need for internal reporting to include options for anonymity. Making reports of wrongdoing can be difficult for some people and providing an anonymous option can make it easier.

We note that East Pilbara's Plan directs staff wishing to make an anonymous complaint to external agencies, either the CCC or the PSC. While directing staff to appropriate external reporting options is important, in our view better practice would be for internal reporting to also have anonymous options.

Entities need to better use information they receive about suspected fraud

None of the entities we reviewed have a way to capture, collate and analyse all information about potential fraud. The Standard expects organisations to develop a program and

[6] Queensland Crime and Corruption Commission 2018 *Fraud and Corruption Control: best practice guide* p49.

[7] Public Sector Commission *2018 State of the sector statistical bulletin*: Integrity and Conduct Survey results.

recommends the development of a fraud register. Capturing information in a central location would make it easier for entities to look for trends, identify issues early and act appropriately.

Entities have reported potential fraud to the CCC. The entities we reviewed told us they had reported 4 instances of potential fraud in the past 5 years.

Audit focus and scope

This audit assessed whether local government entities have taken appropriate steps to prevent fraud. We asked the following questions:

1. Have entities implemented a coordinated approach to manage fraud risks?
2. Do entities have adequate controls for preventing and detecting fraud?
3. Do entities respond appropriately to suspected fraud?

During our audit we considered:

- key principles from the Fraud and Corruption Control Standard (AS 8001-2008)
- guidance issued to entities by the Department of Local Government, Sport and Cultural Industries
- guidance material issued by audit offices in other jurisdictions
- reports published by the CCC and the PSC
- the best practice guide for fraud and corruption control published by the Crime and Corruption Commission in Queensland
- international research.

During the audit we:

- provided a questionnaire to all 148 local government entities, requesting information about approaches to managing fraud risks.
    - 118 entities responded to the questionnaire (see Appendix 3)
    - 91 provided copies of their Codes of Conduct
    - 26 provided copies of their Plans. We reviewed the Plans for key elements of the Standard, including an entity position statement, accountabilities, a fraud risk assessment, outline of key controls, and reporting avenues and protections.
- reviewed approaches in more depth at 5 entities. This included interviews with key staff, and reviews of policies, registers and complaints systems. This sample included entities ranging from relatively small to large, from both metropolitan and regional areas.

We did not conduct detailed reviews of procurement, record keeping or systems for verifying employee identities. These areas were the focus of recent performance audits by this Office.

This was a narrow scope performance audit, conducted under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target entity compliance with legislation, public sector policies and accepted good practice. The approximate cost of undertaking and tabling this audit is $300,000.

Appendix 1: Summary of legislated responsibilities

Entities are required to meet a number of legislated responsibilities that help control fraud risks. A summary of key elements are listed below. This list is not exhaustive.

Legislation	Fraud related requirements
Local Government Act 1995	• disqualifies individuals from becoming elected members due to insolvency, criminal convictions, or misapplication of funds • councils must believe that a person is suitably qualified for the position of CEO, and CEOs must believe that staff are suitably qualified for their positions • all employees must be selected in accordance with the principles of merit and equity • mandates a general need for good government and the creation of a Code of Conduct • council members, the CEO and designated staff members must disclose financial interests' • employees must disclose any interests when they are advising or reporting to council • an audit committee must be formed • sets out penalties for improper use of information
Local Government (Rules of Conduct) Regulations 2007	• requires council members to act ethically, be open and accountable • forbids council members from influencing employees or using their office for personal advantage • council members must declare any interests in matters being discussed at council or audit committee meetings • sets out restrictions on gifts and travel contributions to councillors and requirements for records to be kept
Local Government (Financial Management) Regulations 1996	• CEOs are to establish efficient systems and procedures for collection and custody of money owing to the entity
Local Government (Audit) Regulations 1996	• describes the function of the audit committee • Regulation 17 requires a CEO to review appropriateness and effectiveness of systems and procedures relating to risk management, internal control and legislative compliance. This is then reported to the audit committee
Local Government (Administration) Regulations 1996	• sets out information on disclosure of financial interests • provides detailed information on what value of gifts must be reported and which are prohibited • requires a register of gifts to be publicly accessible • requires Codes of Conduct to contain information on gifts, travel contributions and disclosing interests

Legislation	Fraud related requirements
Local Government (Functions and General) Regulations 1996	• entities must develop a policy for purchases less than, or equal to, $150,000 • purchases worth more than $150,000 must be conducted through tender • sets out requirements for pre-qualified suppliers
Public Interest Disclosure Act 2003	• entities must ○ publish internal procedures for reporting a PID ○ designate at least 1 PID officer to receive reports. They must comply with the Public Sector Commissioner's minimum standards of conduct and integrity

Source: OAG

Appendix 2: Better practice principles

The table below shows key principles on which our audit focused. These principles are not exhaustive. Entities seeking to implement better practice approaches should also consult the Standard, and the guidelines prepared by the Department of Local Government, Sport and Cultural Industries.

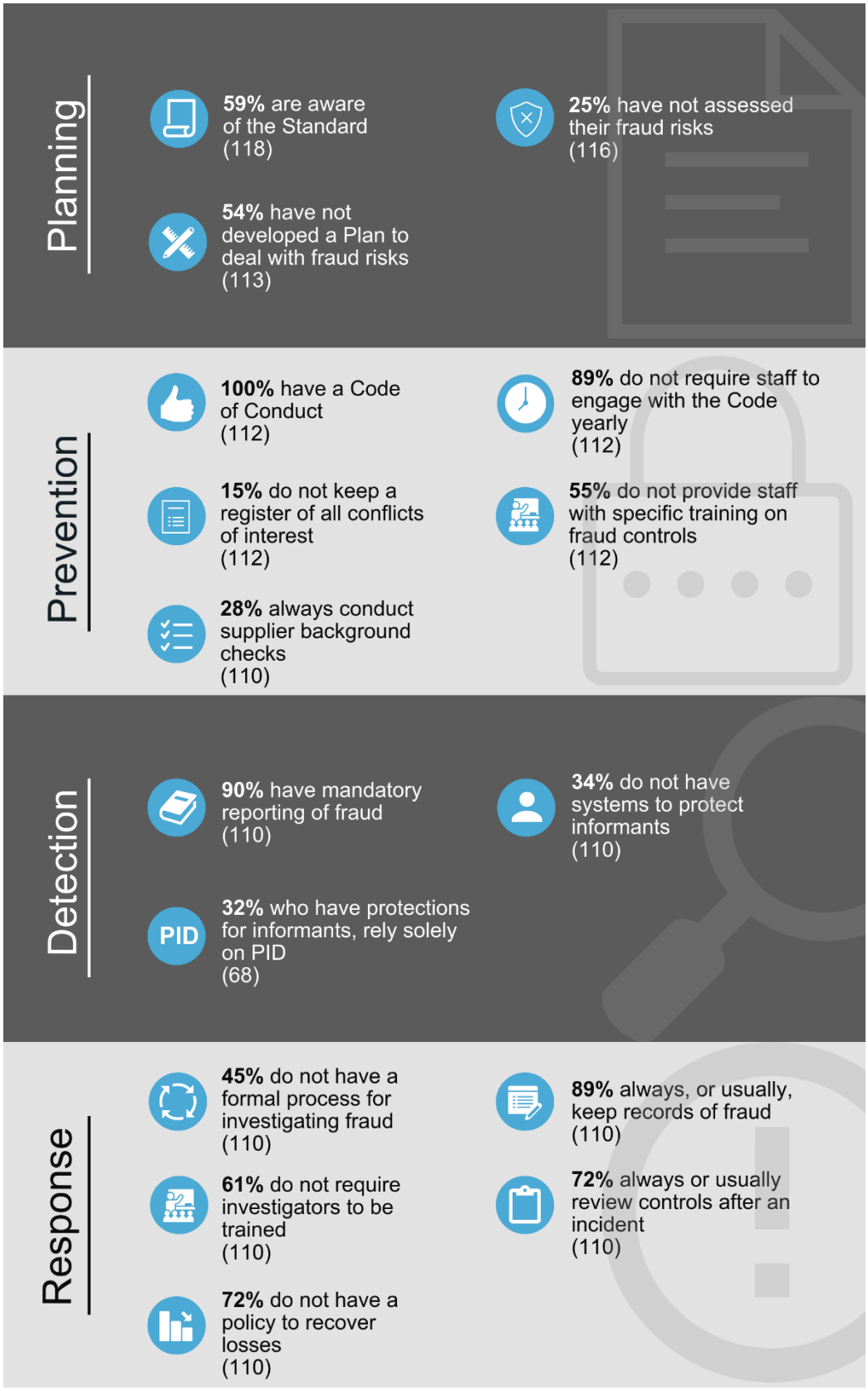
Objective	Principle	What we would expect
Planning Develop a coordinated approach to manage fraud risks	Risks are understood	• Fraud risks across organisation are assessed, documented and controls are in place.
	Approach is documented	• Fraud and Corruption Control Plan (Plan) is in place and reviewed at least once every 2 years.
	Internal audit considers fraud risks	• Audit committee engages with internal audit plan to ensure fraud risks are considered.
Prevention Create a fraud resistant organisation	Policy framework is in place	• Integrity policies (such as Codes of Conduct and conflicts of interest) are appropriate, clearly written and available. • Staff regularly engage with integrity policies. For example, signing yearly an understanding of the Code of Conduct. • Fraud prevention and awareness training, newsletters and presentations are used to communicate entities ethical standards to staff.

	Internal controls are in place	• Business processes, especially those assessed as higher risk, have controls that are well documented, updated and understood by all staff.
		• Entities verify identity and credentials of all new employees and employees transferring to areas of higher risk, including:
		  ○ verify necessary qualifications
		  ○ review of past work history and referee checks
		  ○ criminal background checks
		  ○ confirm professional memberships are valid.
		• Supplier credentials are checked, particularly for high-risk or high value purchases, including:
		  ○ Confirm ABN
		  ○ confirm directors are not bankrupt or disqualified.

Objective	Principle	What we would expect
Detection Entities are ready to detect fraud	Detection systems are in place	• Entities should implement detection systems, as appropriate to their business needs, to identify potential fraud as soon as possible. • Multiple avenues are in place for staff, the public and suppliers to report concerns. • Reporting processes are well advertised, and include anonymous options.
Response Entities are ready to respond to potential fraud	All information is considered	• Entities should implement processes to record, analyse and escalate all incidents. • Processes are in place to review internal controls after incidents.

Source: OAG

Appendix 3: Summary of local government fraud questionnaire results



Number of responses to question marked in (*)

Source: OAG

Appendix 4: Full responses from audited entities

Shire of East Pilbara

Specific responses to recommendations

The Shire of East Pilbara agreed with all recommendations. They provided additional comments on recommendations:

2. Agree. But it is noted that the Shire of East Pilbara does have a Fraud and Corruption Plan. Our priority should be to deploy the plan effectively within the organisation and to undertake regular reviews internally

4. Agree. Conflicts of interest are recorded for elected members and key officers who are writing reports and/or attending Council meetings. It is noted that conflicts of interest for staff need to be recorded and this practice needs to be embedded further within the organisation.

Shire of Katanning

Specific responses to recommendations

The Shire of Katanning agreed with all recommendations.

City of Nedlands

The City is encouraged by the audit work of the Office of Auditor General in the local government space and believes that its work to date in providing clarity on governance inconsistencies and interpretation in local government, which is long overdue.

Specific responses to recommendations

The City of Nedlands agreed with all recommendations and advised they will aim to implement a streamlined and coordinated approach towards risk management within the next 18 months. They provided additional comment on recommendations:

1. Agree. In the past, the City has conducted an organisation wide Risk Assessment program which incorporated a fraud risk assessment. However, the City will aim to undertake the first full fraud risk assessment within next 18 months.

2. Agree. The City will aim to develop and implement a control plan within 8 months.

3. Agree. 2019/20 training will be scheduled followed by annual training.

4. Agree. The City agrees that all conflicts of interest are to be recorded and assessed. At present, the implemented process is to record, assess and manage the declared conflict of interest by the Elected Members and staff for any matter to be discussed at Council meetings. Based on this recommendation the City agrees that procedures should be in place for assessing and recording all conflicts of interest; however, is not aware of the nature, content or need for management plans to achieve this. The City will aim to implement an appropriate Procedure within 8 months.

5. Agree. It is noted that the need for and extent of verification, is a matter to be considered within proper risk assessment, as part of policy and procedures scope. At present, there are verification processes in place for both employees and suppliers. However, there is definitely room for the improvement in this area. Accordingly, the City will aim to review and update its HR and suppliers' policies and procedures within 12 months.

6. Agree. The City will aim to implement this within 12 months.

7. Agree. Once the work around the implementation of streamlined and coordinated approach towards fraud risk management is completed, the City will be able to perform the above task on an ongoing basis.

Shire of Serpentine-Jarrahdale

The Shire of Serpentine Jarrahdale welcomes the findings and subsequent recommendations of the 2019 Performance Audit for Fraud Prevention in Local Governments. It considers that the report is a balanced representation of areas and a good platform to work towards enhanced fraud management activities.

Specific responses to recommendations

The Shire of Serpentine-Jarrahdale agreed with all recommendations. They provided additional comment on recommendations:

1. Agree. The Shire will continue the fraud risk activities scheduled in the Internal Audit – Interim Audit Plan 2019. Outcomes of the initial risk / control activities will be transitioned to the updated Risk Framework when complete. Timeframe: April 2020.

2. Agree. The Shire will build a framework for management of fraud with a view to integrate into ongoing awareness and training processes inclusive of periodic review. Timeframe: April 2020

3. Agree. The Shire is in the process of implementing a learning and development management system. Induction and code of conduct are scheduled to be the initial modules to be implemented. The modules will be required on a periodic basis and be supported with audit trails and electronic signatures for tracking attendance. Timeframe: December 2019.

4. Agree. Building upon processes implemented to capture all conflicts of interest, the Shire is in the process of rolling out a consistent conflict of interest awareness process and supporting policy / procedure environment. Once the learning and development management system is implemented the Shire will progress to implement a specific module within the system. Timeframe: April 2020.

5. Agree. Employees - Policies will be reviewed to document a risk based approach to the screening of employees including enhancing the approach to assess qualifications, references and background searches. Suppliers - Policies will be reviewed to document a risk based approach to the screening for suppliers including consideration of legal history and checking of supplier Directors. Timeframe: December 2019.

6. Agree. Whistle-blower processes are scheduled to progress. The scope and approach of the processes will be informed by the recommendations of the report. Timeframe: October 2019.

7. Agree. Whistle-blower processes are scheduled to progress. The scope and approach of the processes will be informed by the recommendation of the report. April 2020.

City of Vincent

The City of Vincent (City) accepts the finding in the report and acknowledges that there are gaps in the City's current management and reporting of potential fraud. The City will table the Summary of Findings to its Audit Committee in August 2019, along with a management plan to address the recommendations identified. The management plan will be monitored by the Audit Committee to ensure all items are adequately completed.

Specific responses to recommendations

The City of Vincent agreed with all recommendations. They provided additional comment on recommendations:

1. Governance will develop and implement a program for the annual review of fraud risks across the business. The proposed implementation date is June 2020. The findings of the annual review will be tabled at Audit Committee, with any items requiring action being included in the Audit Log and monitored by the Audit Committee until completion.

2. Governance will review the City's current Fraud and Corruption Prevention Policy and prepare a control plan which incorporates this policy. The proposed implementation date for the plan is June 2020. The plan will be reported to Audit Committee annually and updated as required.

3. Human Resources with the support of Governance will develop and implement an online fraud awareness training program to be completed by all staff. New staff will be required to complete the training as part of their online induction process and current staff will receive notification to complete the training annually via the induction portal. The proposed implementation date is January 2020.

4. The City currently has a register for Elected Members and senior staff as required by the Local Government Act 1995 and a register to capture and manage any other actual, perceived or potential staff conflicts of interest. Governance, in coordination with Human Resources, will ensure all staff are aware of the conflict of interest disclosure requirements and provide training for new staff as part of the induction process.

5. Human Resources will develop and implement a recruitment and selection policy and procedure (which will include identity and integrity checks) for the City. Human Resources will periodically monitor employees for change of circumstances via a declaration form which WALGA are currently preparing to supply to Local Governments. The proposed implementation date is January 2020. Finance will review and update the City's supplier verification process. The proposed implementation date is December 2019.

6. The City will investigate systems and processes to report any potential fraud, including anonymous reporting. The proposed implementation date is December 2020.

7. The fraud reporting system, as referred to in 6. above, should enable this data to be easily compiled. Governance will periodically review the data.

Auditor General's reports

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
Serving the Public Interest

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