Audit Committee Meeting

Attachments

21 July

2022

Western Australian
Auditor General's Report

Fraud Risk Management – Better Practice Guide

Report 20: 2021-22
22 June 2022

Office of the Auditor General
Western Australia

Report team:
Carl Huxtable
Chiara Galbraith

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

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

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

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Fraud Risk Management – Better Practice Guide

Report 20: 2021-22
June 2022

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

FRAUD RISK MANAGEMENT – BETTER PRACTICE GUIDE

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

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

CAROLINE SPENCER
AUDITOR GENERAL
22 June 2022

Contents

Auditor General's overview

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

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

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

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

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

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

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

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

Part 1: Introduction

1.1 About this guide

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

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

1.2 Who should use this guide

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

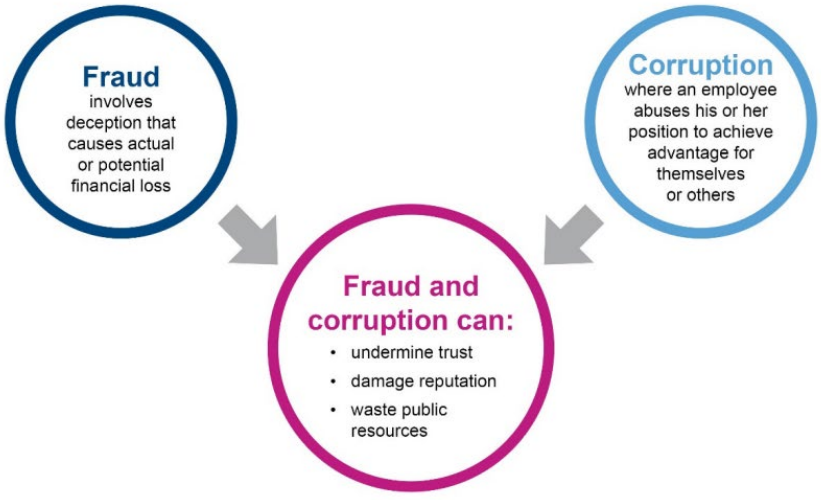
Parts 1 and 2 are intended for directors general, chief executive officers, managers and other key decision makers. Part 1 outlines the high-level principles entities should apply to fraud and corruption risk management and Part 2 highlights the importance of entities implementing an effective fraud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

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

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

1.3 What is fraud and corruption

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



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

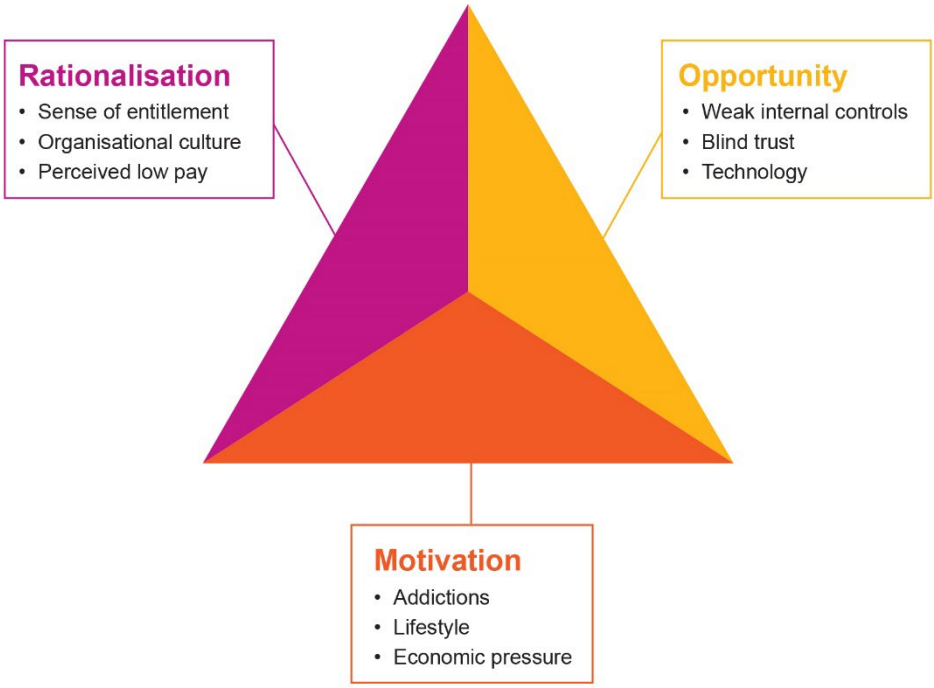
Figure 1: Definitions of fraud and corruption

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

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

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

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



Source: OAG adapted from Other People's Money[1]

Figure 2: The fraud triangle

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

1.4 Fraud control principles

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

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

Strong leadership	An entity's leadership must model a commitment to fraud control, establishing a strong 'tone at the top' culture to demonstrate their personal commitment to operating with integrity and encouraging a 'finding fraud is good' mindset.
Recognise fraud as a business risk	Entities must acknowledge they are vulnerable to fraud. Fraud should be viewed and treated in the same way as an entity's other enterprise risks.
Adequate control resourcing	Entities should invest in appropriate levels of fraud control resourcing including specialist information system security management personnel.
Clear accountability for fraud control	Entities should establish clear personal accountabilities for fraud control at the governance, executive management and management levels.
Implement and maintain an effective fraud control system	An effective fraud control system (FCS) can reduce the opportunity for fraud. It needs to align with better practice guidance, be fully implemented, monitored and updated periodically.
Periodic assessment of fraud risks	Fraud risk assessments should be carried out periodically or whenever a significant change that affects the entity occurs.
Effective awareness raising program across the entity	To ensure employees recognise red flags for fraud, entities should establish an effective awareness program.
Open channels to report suspicions of fraud	To encourage whistle-blowers to come forward entities should support: • active reporting of fraud through accessible anonymised reporting channels • ensure that the entire workforce is aware of organisational expectations for reporting detected or suspected cases of fraud • ensure they have robust whistle-blower protection policies and procedure that includes assurance that victimisation of those who, in good faith, make such reports will not be tolerated.
Implement a fraud detection program	An effective fraud detection program that includes detection measures such as data analytics and post-transactional review are important.
Consistent response to fraud incidents	Rapid and robust response to suspected fraud events with effective investigation procedures will drive decisive action and result in better outcomes for detected fraud incidents. A strong and consistent response to all fraud events will send a strong message to the workforce that the entity will not tolerate fraud, no matter how minor.

Source: OAG

Table 1: Foundation principles for fraud control

1.5 Acknowledgements

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

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

Part 2: Why develop a fraud risk management program

2.1 Overview

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

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

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

2.2 Public sector requirements

Entities are required to consider their risks and implement protections.

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

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

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

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

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

2.3 Impact of fraud in the WA public sector

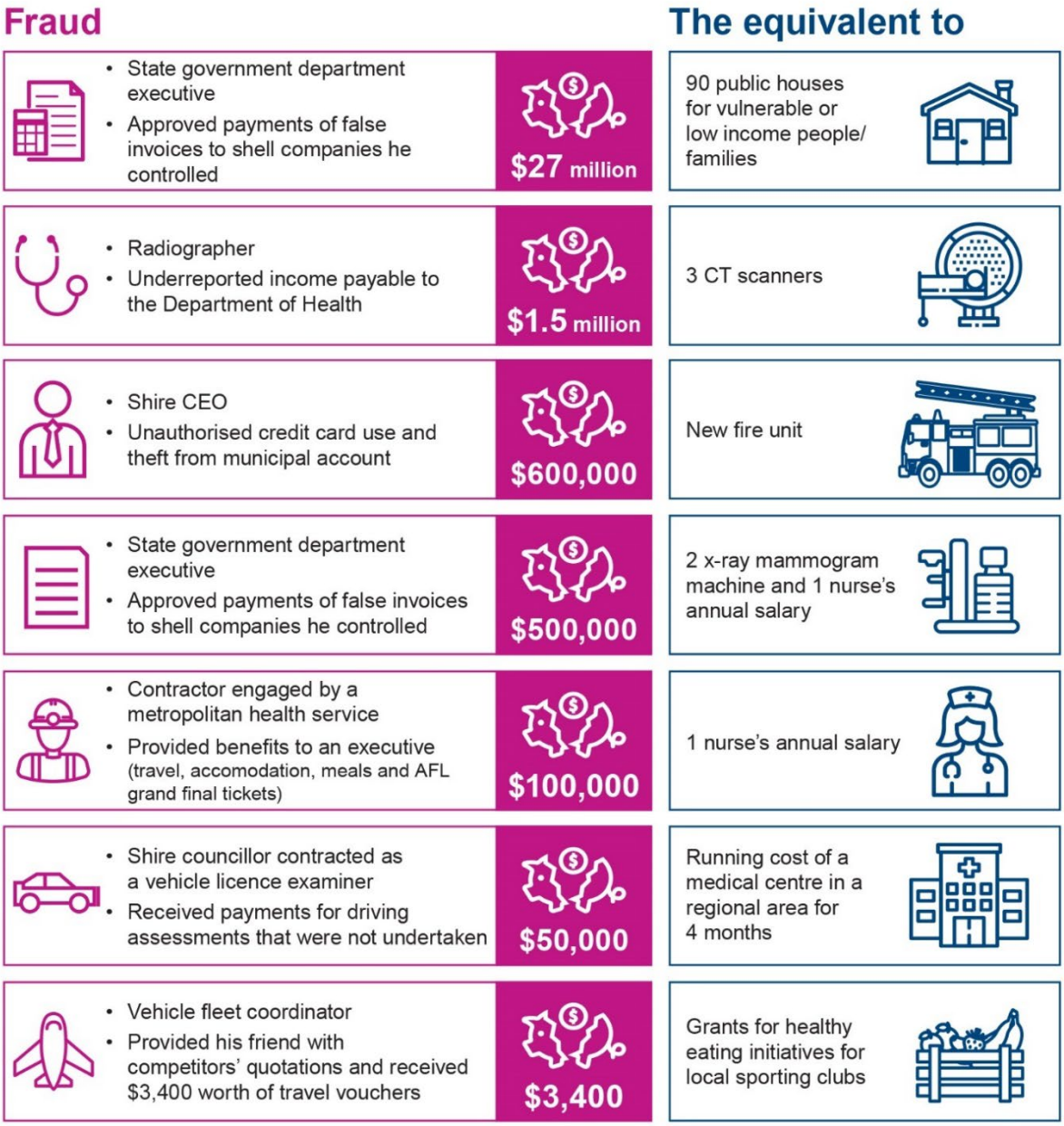
The Association of Certified Fraud Examiners Report to the Nations 2022, estimated that fraud losses in businesses, government and not-for-profits are approximately 5% of their

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

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

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

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



Source: OAG

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

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

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

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

2.4 Status of fraud control maturity across the sector

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

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

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

Source: OAG

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

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

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

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

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

Source: OAG

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

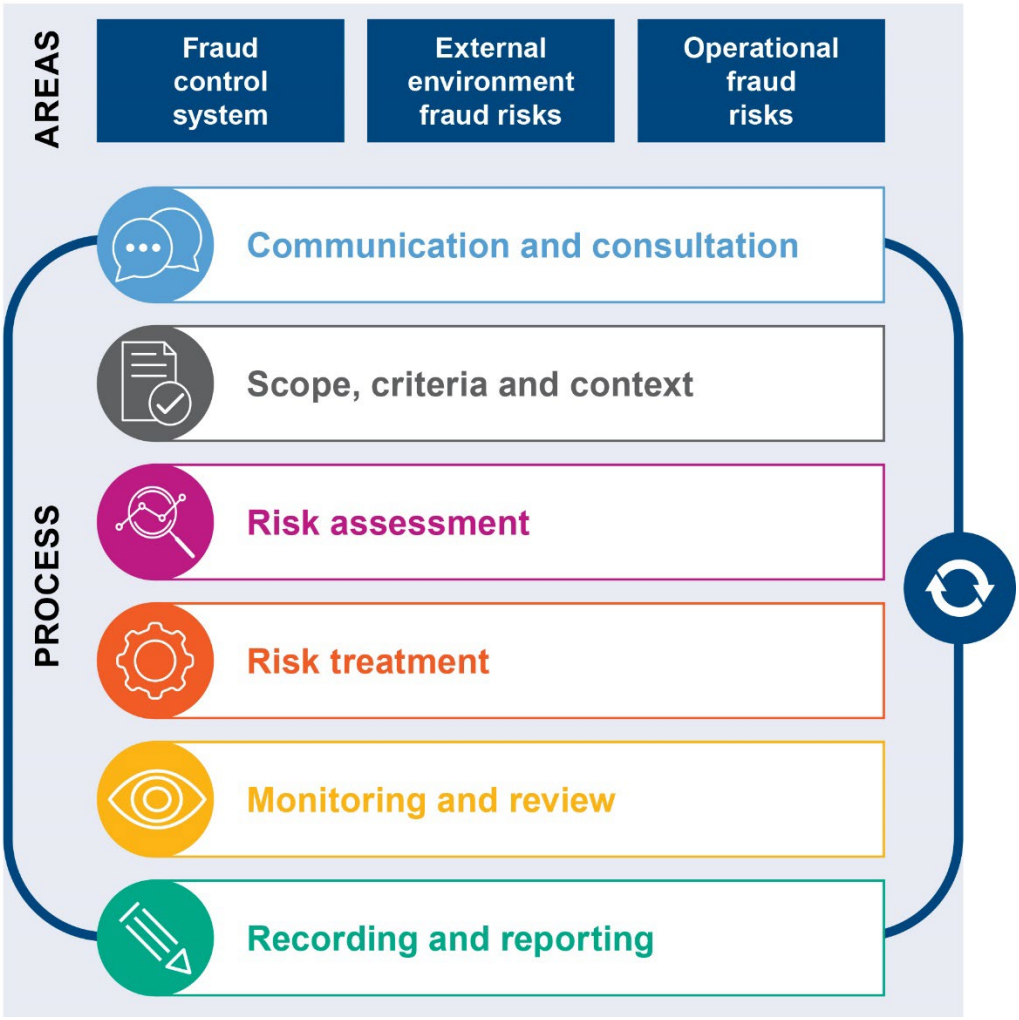
Part 3: How to develop a fraud risk management program

3.1 Overview

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

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

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



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

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

3.2 Where to look for fraud vulnerabilities

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

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

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

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

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

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

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

Table 4: Elements of a fraud control system

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

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

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

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

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

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

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

Table 5: External factors that can impact an entity

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

3.3 Fraud risk management process

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

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

Communication and consultation

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

Communication and consultation are intended:

"…to assist stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required."[5]

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

Communication and consultation	Better practice
Promote awareness and understanding of fraud risks	• Implement multimodal training programs specific to fraud risks – "What is a fraud risk" • Effectively communicate to employees that the objective is to protect the integrity of the entity and employees
Bring different expertise together throughout the process using effective mechanisms	• Engage different levels of expertise and experience to bring various perspectives • Use a variety of communication methods such as emails, workshops, one-on-one interviews and surveys to obtain a wide range of feedback and opinions
Build a sense of inclusiveness and ownership for process owners (e.g. one-on-one interviews, focus groups)	• Use fraud risk workshops to obtain "buy in" from process operators and owners • Invite all relevant employees, regardless of seniority, to attend a workshop
Obtain sufficient knowledge from relevant stakeholders of business processes to facilitate fraud oversight and decision making	• Facilitate fraud risk workshops to discuss and map business processes and internal controls • Ask attendees to consider "what could go wrong?" in processes they engage with or manage • Identify areas of fraud risk in a process map that requires internal controls
Engage with relevant stakeholders to obtain feedback and information to support decision-making	• Structure emails and/or surveys that focus on fraud risks for specific processes • Adopt appropriate modes of communication

Source: OAG

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

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

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

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

Scope, context, and criteria

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

> *"…Scope, context and criteria involve defining the scope of the process and understanding the external and internal context."*[6]

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

Factor	Procure to Pay

Scope	• The specific parts of the Procure to Pay process to be assessed are: supplier selection, onboarding vendors, purchase validation (business case, receipt of goods/services) and release of payment.
	• We will engage with the finance business unit and operational staff responsible for purchase orders and validation of receipt of goods/service.
	• The entity's risk assessment policy dated 31 January 2020 will be applied in conjunction with the approved fraud risk assessment program dated 30 June 2021.
	• As the entity's procurement staff are across the State, we will need to engage in a number of online meetings with potential site visits.
	• Timeline:
	  ○ engagement with procurement staff by 30 June 2022
	  ○ identification of risks by 31 October 2022
	  ○ completion of risk register and mapping of risks by 31 December 2022
	  ○ first review to Internal Audit and Risk Committee (IARC) by 28 February 2023
	  ○ second review to IARC by 30 April 2023
	  ○ submission to Board for approval by 31 May 2023.

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

Context	Internal factors include: • the strategic objectives of the entity are: community focused delivery of services, sound business practices and quality services. A list of the specific goods, services or works to be procured are provided in Annexure A • the existing employee level in the Procure to Pay process is sufficient, however, their experience is inadequate. No training has been delivered in identifying indicators of potential fraud • there is no assessment of fraud controls within vendors • the entity has policies and processes in respect of independence for supplier selection panels and purchase validation. External factors include: • increasing fraud trends targeting procurement and finance teams (i.e. business email compromise ‐ fake emails impersonating an internal senior person or a vendor) • recent known scams in the public domain that have been uncovered.
Criteria	• The below risk criteria are taken from the entity's risk assessment policy dated 31 January 2020. • The entity rates likelihood risk on a scale from extremely unlikely to almost certain. Within the Procure to Pay process, rare is conceivable but unlikely, unlikely is conceivable and has occurred in the past but unlikely in the next year. • The entity rates consequence risk on a scale from negligible to catastrophic across the following loss factors: financial, reputational, legal, service delivery. • Within the Procure to Pay process, negligible has no negative consequence, low disrupts internal non-management process and has no external financial loss, moderate requires corrective action by senior management, potential disciplinary action and minor financial impact etc.

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

Scope, context and criteria	Better practice
Define the scope of the activity being assessed for fraud risk including objectives and decisions to be made prior to commencing any fraud risk assessment	• Clearly document the scope and objective of the process that is being assessed for fraud risks • Circulate a document that sets out the scope to all employee participating in the fraud risk assessment • Break down complex processes into manageable scopes

Scope, context and criteria	Better practice
Establish the context of the fraud risk activity	• Understand the external environment • Understand the internal operating environment • Reflect the specific environment of the activity to which the fraud risk management process is to be applied
Align the fraud criteria with an overarching risk management framework used to assess all business risks for consistency	• Review the entity's existing risk management framework prior to commencing to ensure up-to-date and fit-for-purpose • Align consequence and likelihood criteria and the risk rating matrix with existing framework
The fraud risk assessment criteria should reflect the organisation's values, objectives and resources and be consistent with policies and statements about risk management	• Review the entity's existing risk management policy to understand the entity's risk appetite

Source: OAG

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

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

Risk assessment

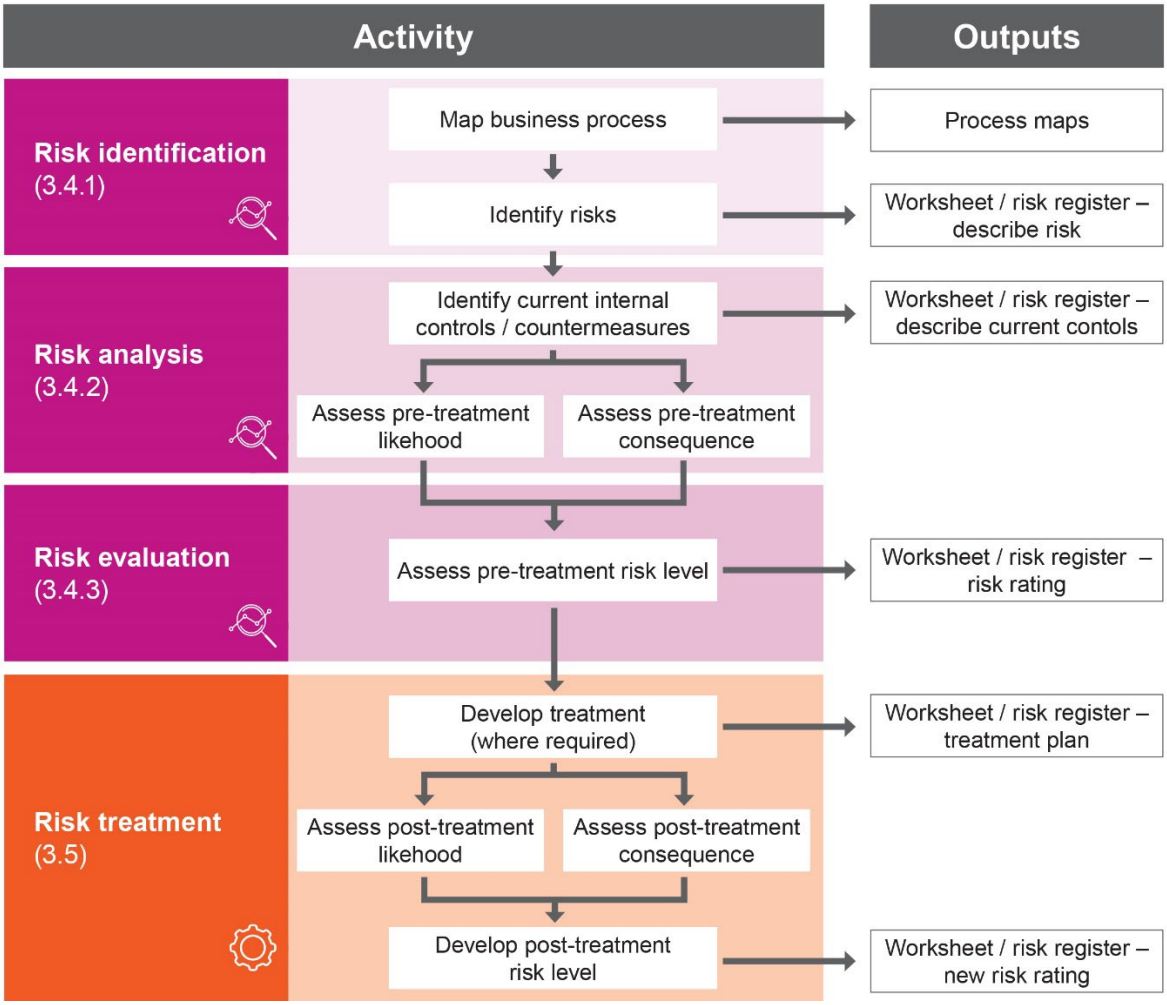
Once the scope, context and criteria are established, entities need to assess their fraud risks.

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

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

- risk identification
- risk analysis
- risk evaluation.

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



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

Figure 5: Risk assessment and treatment stages overview

Identifying risks

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

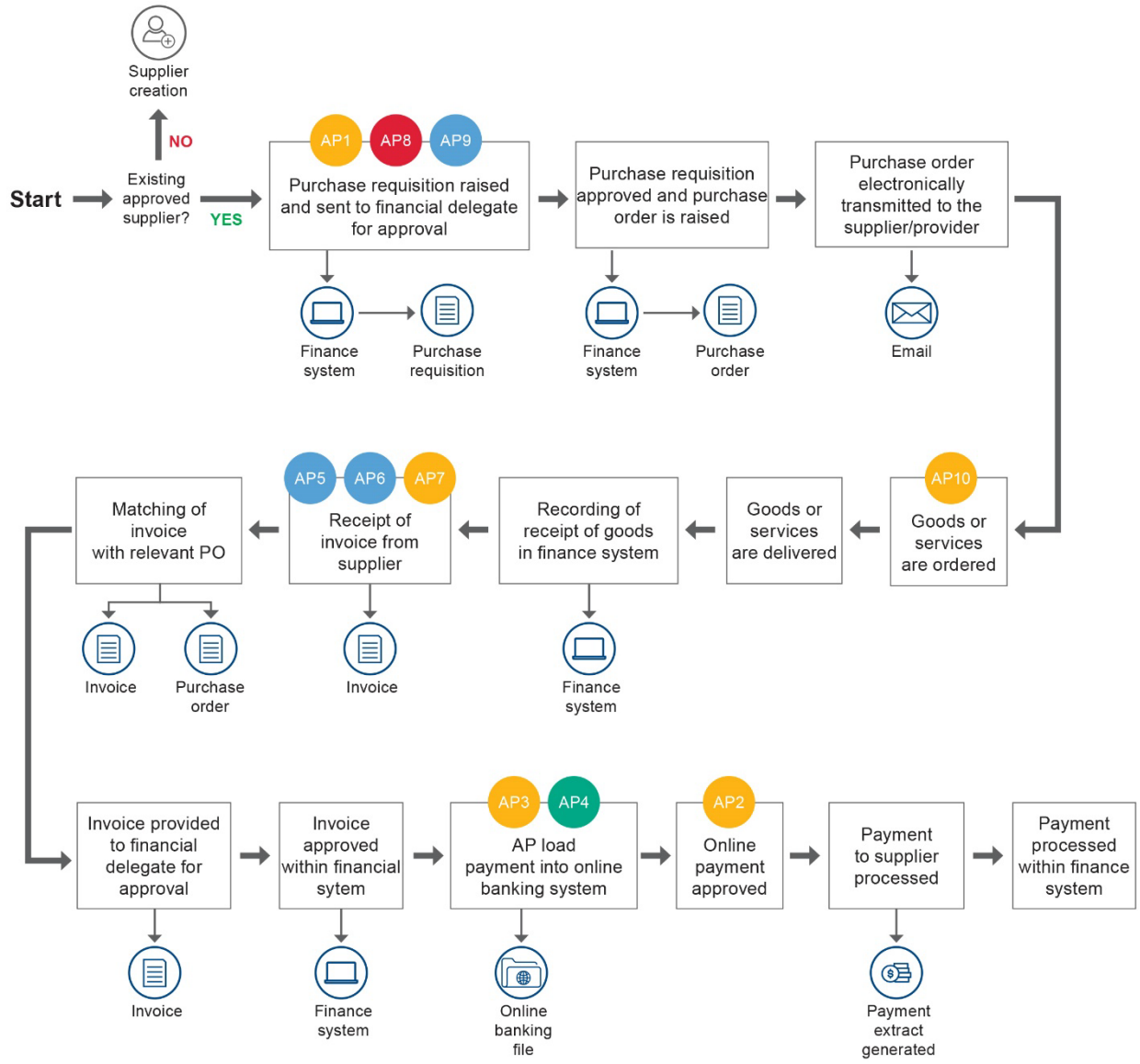
Risk identification involves:

"… finding, recognising and describing risks that might help or prevent an organisation achieve its objectives."[7]

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

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

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



Source: OAG

Figure 6: Accounts payable process map

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

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

Finally, a good fraud description will allow you to understand ways to prevent or detect the fraud. One way to identify and describe your fraud risks is to consider who did what and what the result was, also described below as the Actor, Action, Outcome method[8]:

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

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

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

Appendix 5.3 includes:

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

Analysing fraud risks

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

Risk analysis is:

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

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

An analysis of each risk includes considering:

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

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

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

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

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

Source: OAG

Figure 7: Example of a risk assessment matrix

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

Risk analysis	Better practice
Consider uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness	• Detailed documentation of the analysis including reasoning for decisions for example if a risk is determined to be HIGH for consequence document why and what inputs were used
Events can have multiple causes and consequences and affect multiple objectives	• Deep dive analysis to identify all causes, both internally, externally and potential consequences
Scrutiny of existing controls	• Sufficiently analyse and test existing controls including walk-throughs and penetration testing • Consider engaging specialists to identify gaps in existing system controls

Source: OAG

Table 8: Better practice examples of the risk analysis stage

Evaluating fraud risks

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

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

The purpose of risk evaluation is to:

"… support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required." [10]

It is important that the evaluation of fraud risks involves detailed input from the process and risk owners and includes senior employees who can consider the cost of countering fraud against the entity's risk tolerance. The evaluation considers the residual fraud risk and should conclude with one of the following outcomes[11]:

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

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

Risk evaluation	Better practice
Evaluate results from risk assessment	• Comparing the results of the risk analysis with the established risk criteria to determine if and where additional action is required
Record and communicate evaluation results	• Risk evaluation outcomes are recorded, communicated and then validated at appropriate levels of the organisation

Source: OAG

Table 9: Better practice examples of the risk evaluation stage

Risk treatment

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

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

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

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

The aim of risk treatment is to:

".. select and implement options for addressing risk."[12]

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

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

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

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

Risk treatment	Better practice
Determine appropriate risk treatments	• Select risk treatment options with the entity's objectives, risk criteria and available resources • Balance the potential benefits against cost, effort or disadvantage of implementation
Document implementation plan	• Document the treatment plan outlining the responsibilities, resources and other relevant implementation information in the fraud risk worksheet
Risks that do not have a treatment option	• If no treatment options are available or if treatment options do not sufficiently modify the fraud risk, the risk is recorded and kept under ongoing review
Remaining risk is documented	• Inform decision makers and other stakeholders of the nature and extent of the remaining risk after treatment • Document the remaining risk and subject to monitoring, review and, where appropriate, further treatment
Consider beyond economic consequences	• Justification for risk treatment is broader than solely economic consequences and considers the entity's obligations, voluntary commitments and stakeholder views

Source: OAG

Table 10: Better practice examples of the risk treatment stage

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

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

Monitoring and review

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

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

Monitoring and review is:

"… to assure and improve the quality and effectiveness of process design implementation and outcomes."[13]

Monitoring and review	Better practice
Monitoring and review takes place during all elements of fraud risk management program	• Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback
Monitoring and review progress is reported	• Results of monitoring and review are incorporated throughout the entity's performance management, measurement, and reporting activities

Source: OAG

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

Recording and reporting

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

Risk management process and its outcomes should be:

"… documented and reported through appropriate mechanisms."[14]

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

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

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

Recording and reporting	Better practice
Detailed recording of fraud risk assessment process	• Worksheets include adequate information that demonstrates reason for decisions made and actions taken
Ongoing monitoring and periodic review of the fraud risk management process and its outcomes is planned, and responsibilities clearly defined	• Updates provided to senior management and those charged with governance on progress • Monitoring through audit committee • Documented responsibilities for undertaking fraud risk management are outlined in the entities' FCS

Source: OAG

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

Conclusion

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

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

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

Appendix 1: Glossary

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

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

Appendix 2: References

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

Appendix 3: Fraud control system benchmarking tool

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

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

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

Step 1	Consult and collaborate across the entity in a consideration of the FCS benchmarking model and determine which, if any, elements of the model are not relevant to the entity's own circumstances, make necessary adjustments to the model in preparation for analysis.[15]
Step 2	Gather all entity documentation pertaining to the control of fraud risk within the entity – this would include: • current FCS documentation • current governing body charter • most recent fraud risk assessment • the entity's disciplinary procedures • recent analysis of awareness raising activities within the entity • most recent external environmental scan analysis

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

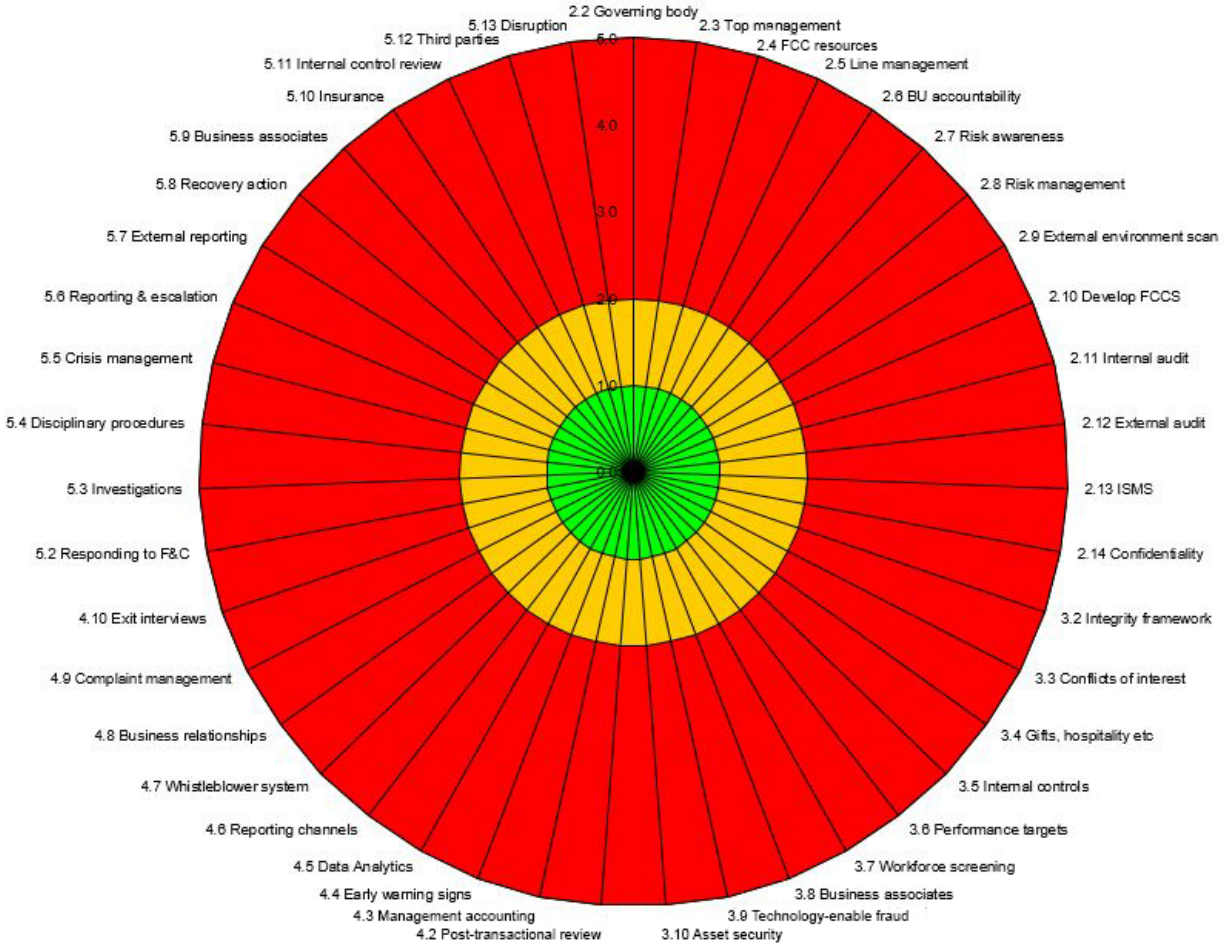
	• internal audit charter • any recent internal audit reports in relation to fraud risk management • all integrity related documentation • current workforce screening policy • current cybersecurity / information system management policies • a summary of the last 5 years fraud incidents covering results could provide insight into common activities, themes and weaknesses. Details such as number of events per year, fraud theme (procurement, CC etc), quantum, fraud substantiated Y/N, vulnerability identified, how vulnerability treated, date vulnerability treated • reports of analysis of internal control efficacy including pressure testing transactions.
Step 3	Consult broadly across the entity to arrive at a realistic and reliable assessment of the entity's current performance against each relevant element of AS8001:2021. Consultation would include: • if a relevant policy or procedure is currently in place or is proposed • the frequency of review of all relevant policies and procedures • if there is adequate resourcing to ensure that the FCS is properly and effectively administered • the culture within the entity in terms of adherence to the key elements of the FCS.
Step 4	Collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its current alignment with AS 8001:2021.
Step 5	Consult broadly within the organisation in relation to initiatives currently in train for implementation in the future, collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its future alignment with AS 8001:2021 on the assumption that the initiative is fully implemented.
Step 6	Enter scores into the model and review the output chart.
Step 7	Present to the relevant oversight committee within the entity.
Step 8	Implement remedial action required for the entity to better align with the better practice model per AS 8001:2021.
Step 9	Monitor the ongoing efficacy of the FCS in light of this analysis over time.

Presentation of the benchmarking analysis

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

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

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



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

Appendix 4: External threat assessment tool

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

Step 1: Consult and collaborate across the entity, make necessary adjustments to the worksheet in preparation for analysis.

Step 2: Gather all documentation pertaining to external threats in the environment in which the entity operates or is considering operations.

Step 3: Consider the most recent fraud risk assessment conducted in relation to the entity's operation.

Step 4: In collaboration with risk and process owners, consider the six PESTLE factors that could impact the entity's fraud risks.

Step 5: Identify external factors that need to be addressed by the entity to more effectively control fraud risks.

Step 6: Develop risk treatments for risks that need to be further mitigated and adjust in fraud risk assessment and fraud control system.

Step 7: Review external threats periodically.

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

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
Political			
To identify the political situation of the country in which the organisation operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and international political pressure.	1. Has there been a recent change in government (at local, state or federal level)? 2. Is there any anticipated change in government funding foreshadowed? How will a change in funding impact the entity's fraud exposure (e.g. an increase in funding for grants or a decrease in funding for administration)? 3. Is there any legislative change anticipated in relation to employment law that may impact the entity's ability to manage its fraud exposure?	Insert text	Insert text

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	4. Is there a likely increase or reduction in government mandated regulation? 5. If yes, will that give rise to an increase in the entity's fraud exposure (either internally or externally initiated fraud)? 6. Are there any other political factors the entity should consider?		
Economic			
To determine the economic factors that could have an impact on the organisation, including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.	1. Are all economies in which the entity operates currently stable? 2. If there are indications of instability in an economy in which the entity operates, to what degree will this impact the risk of fraud within or against the entity? 3. Are there any key economic decisions (either recently implemented or in contemplation) likely to have an impact on the entity's fraud exposure (e.g. rising interest rates, a change in taxation rates)? 4. Is there currently significant pressure on wages and salaries that could act to reduce disposable income of the general population and to what degree could that impact on the entity's fraud exposure? 5. Is there likely to be a change in employment levels in the economy in the next three to five years?	Insert text	Insert text

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

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

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	workforce? 5. Are there any other legal factors that the entity should consider?		
Environmental			
To identify how local, national and international environmental issues are affecting or could affect the organisation.	1. Does the entity operate in circumstances where there is a likelihood of a high environmental impact? 2. If so, does this give rise to any raised risk of manipulation of financial or non-financial reporting? 3. Are there any other environmental factors that the entity should consider?		

Appendix 5: Tools to support the fraud risk management process

A5.1 Communication and consultation tool

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

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

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

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

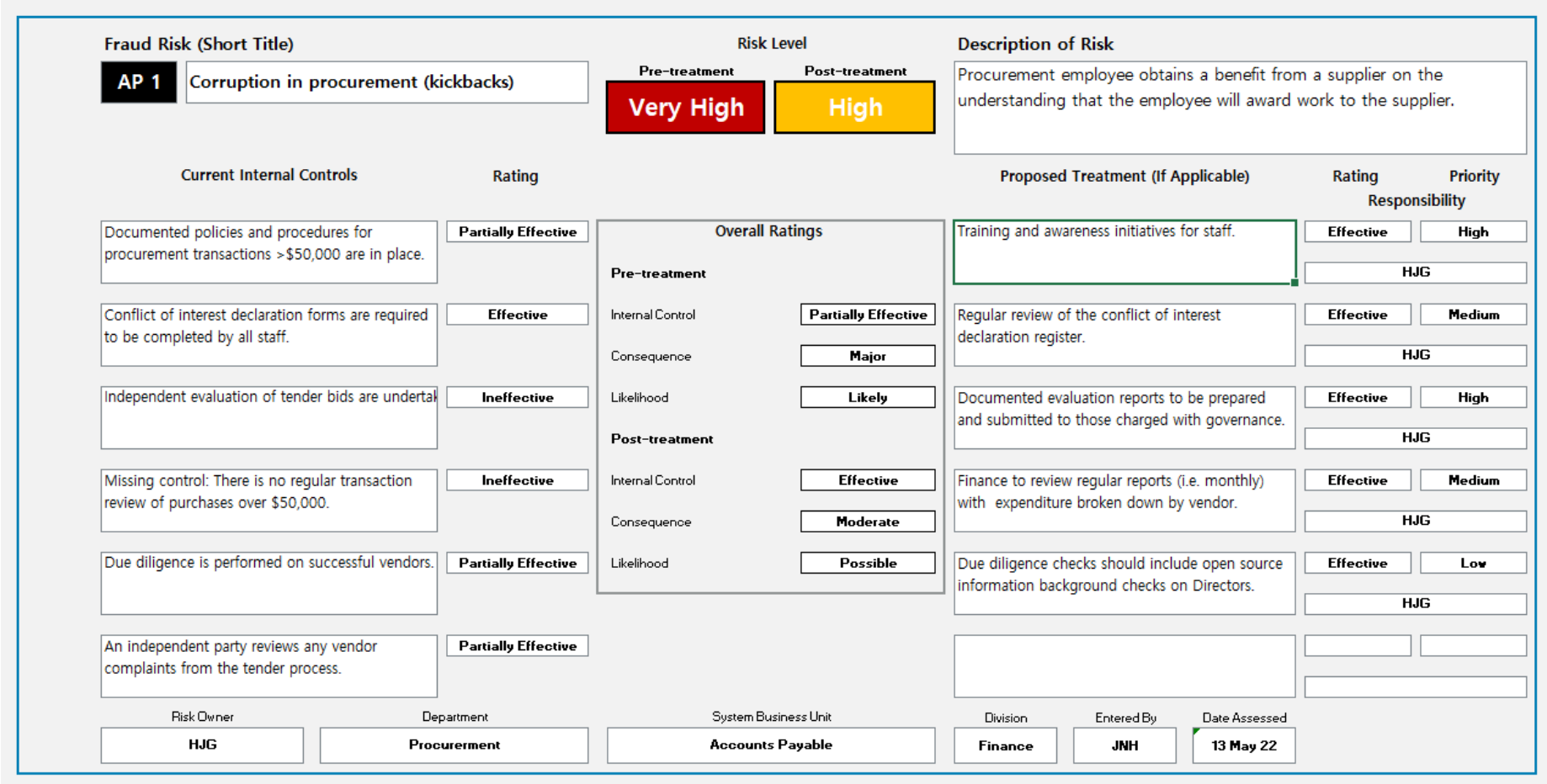
A5.2 Scope context and criteria tool

Factor	Definition	Fraud risk assessment "XX Process"
Scope	The boundaries within which the fraud risk assessment will take place.	• The specific parts of the XX process to be assessed for fraud risks. • The business units and operational teams involved in the processes to be assessed. • Tools to be used in the fraud risk assessment. • Logistical considerations, milestones and timelines for completing the fraud risk assessment.
Context	The internal and external factors influencing the environment the entity operates in.	Internal factors may include: • The strategic objectives of the entity and how this influences the XX process. • The existing employee level in the XX process and their experience, as well as their level of training in identifying indicators of potential fraud. External factors include: • Increasing fraud trends targeting XX process. • Recent known scams in the public domain that have been uncovered.
Criteria	Likelihood and consequence criteria aligned to an entity's existing risk framework that can be used to rate fraud risks identified in the fraud risk assessment.	• Likelihood criteria is a rating scale (i.e Extremely unlikely to Almost certain) set by the entity to identify the expected frequency of a fraud risk in the XX process being realised, both with no internal controls in place (inherent) and existing controls in place (residual). • Consequence criteria is a rating scale (Low – Catastrophic) across a number of defined loss factors (i.e. financial damage, reputational damage, legal damage), to identify the expected impact of a fraud risk in the XX process being realised both with no internal controls in place (inherent) and existing controls in place (residual). • What is acceptable frequency / consequence.

A5.3 Risk assessment tools

A5.3.1 Example fraud risk assessment worksheet

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



Fraud Risk (Short Title)		Risk Level: Pre-treatment	Risk Level: Post-treatment	Description of Risk
AP 1	Corruption in procurement (kickbacks)	Very High	High	Procurement employee obtains a benefit from a supplier on the understanding that the employee will award work to the supplier.

Current Internal Controls	Rating	Proposed Treatment (If Applicable)	Rating	Priority / Responsibility
Documented policies and procedures for procurement transactions >$50,000 are in place.	Partially Effective	Training and awareness initiatives for staff.	Effective	High / HJG
Conflict of interest declaration forms are required to be completed by all staff.	Effective	Regular review of the conflict of interest declaration register.	Effective	Medium / HJG
Independent evaluation of tender bids are undertal	Ineffective	Documented evaluation reports to be prepared and submitted to those charged with governance.	Effective	High / HJG
Missing control: There is no regular transaction review of purchases over $50,000.	Ineffective	Finance to review regular reports (i.e. monthly) with expenditure broken down by vendor.	Effective	Medium / HJG
Due diligence is performed on successful vendors.	Partially Effective	Due diligence checks should include open source information background checks on Directors.	Effective	Low / HJG
An independent party reviews any vendor complaints from the tender process.	Partially Effective			

Overall Ratings	
Pre-treatment	
Internal Control	Partially Effective
Consequence	Major
Likelihood	Likely
Post-treatment	
Internal Control	Effective
Consequence	Moderate
Likelihood	Possible

Risk Owner	Department	System Business Unit	Division	Entered By	Date Assessed
HJG	Procurement	Accounts Payable	Finance	JNH	13 May 22

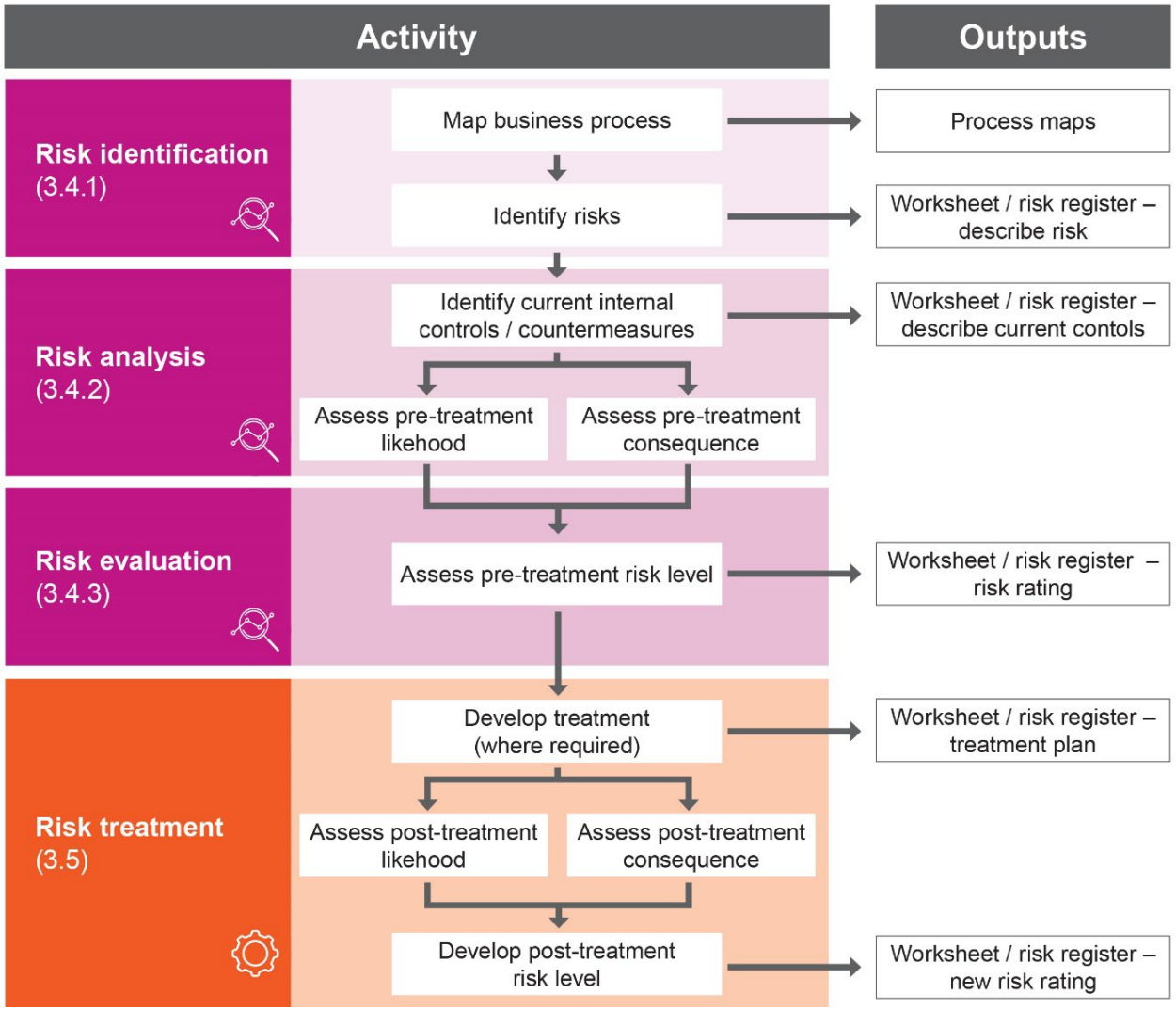
The following is a short summary of the information that would be recorded on each risk assessment sheet (note that much of the information referred to in the following table will not have been prepared in the risk identification stage when the fraud risk worksheet is first created. The worksheet is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

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

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

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

A5.3.2 Risk assessment and treatment process overview



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

A5.3.3 Key fraud risk identification questions

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

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

A5.3.4 Commonwealth Fraud Prevention Centre's 'Actor, Action, Outcome' method of describing fraud risks[16]

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

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

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

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

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

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

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

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

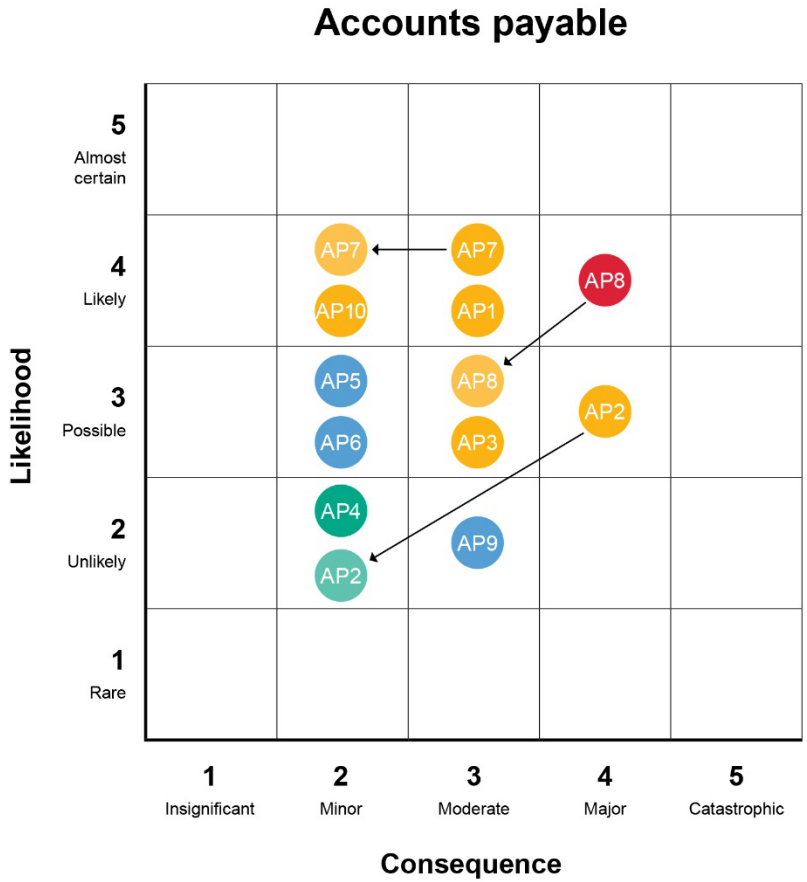
- splitting the authorising powers (submit and process)
    - segregation of duties between invoice entry and payment authority
- validating the invoice details (fictitious invoice)
    - third party verification of goods/services being received
    - check supplier details in your supplier master file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

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

A5.3.5 Example diagrammatic presentation of assessed fraud risks

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

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



Risk rating

- Very high
- High
- Medium
- Low

AP 1	Corruption of the procurement process (kick-backs)
AP 2	Fraudulent alteration of EFT upload file
AP 3	Fraudulent change to existing vendor masterfile record (internal)
AP 4	Fraudulent change to existing vendor masterfile record (external)
AP 5	False invoicing (internal)
AP 6	False invoicing (external)
AP 7	Double invoicing (initiated by supplier/vendor)
AP 8	Collusive tendering (external)
AP 9	Serious/unresolved conflict of interest
AP 10	Fraudulent use of the corporate purchasing card (personal benefit)

A5.3.6 Example public sector fraud risks

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

Accounts payable fraud	
False invoicing (creation of a fictitious vendor)	A fictitious vendor is created in the finance system to which payments for false invoices are made for goods/services not ordered and not delivered (typically fraud of this type involves personnel within the entity but it can be perpetrated at times by external parties acting alone or by external parties operating in collusion with a member of the target entity's workforce)
Fraudulent change to vendor master file	Fraudulent change to the entity's vendor master file (i.e. change of bank details to divert legitimate vendor payments to an account controlled by the perpetrator) – this can be done by a person internal to the entity, a person external to the entity or by collusion between internal and external persons
Online banking fraud	Manipulation of vendor or other payments in the online banking system immediately prior to execution of the payment file in the entity's online banking system – the fraudulent manipulation of the online payment file is concealed by making false entries in the entity's accounting records
False invoicing (existing vendor)	Manipulation and processing of fraudulent payments for invoices apparently rendered by a legitimate vendor but, in fact, fraudulently generated and issued by the perpetrator who is generally a member of the entity's own workforce
Duplicate payments for the invoices already settled	More than one payment is made for the same invoice – this can be initiated inadvertently by a vendor who issues the same invoice twice in error but the vendor then fails to report the double receipt and fraudulently converts the duplicate payment

Procurement and tendering	
Corruption of the procurement process (involving personnel within the entity)	Corruption involving an employee of the entity and a vendor in the selection of a winning bid or tender often involving bribery / kickbacks but often motivated by personal or family association between the bidder and the entity's employee without direct financial reward – corruption can involve provision of a confidential bid price, contract details or other sensitive information to gain an advantage for one tenderer over other tenderers
Bid rigging (excluding personnel within the entity)	Collusive tendering between multiple bidders for the same contract for mutual advantage (no involvement of the entity's personnel)

Procurement and tendering	
Conflicts of interest	Undeclared association between an employee of an entity and a tenderer giving rise to an actual or perceived bias in awarding of a contract
Improperly receiving hospitality, gifts and benefits	An employee receiving or soliciting hospitality, gifts or benefits from a vendor or potential vendor hoping to gain a commercial advantage in doing so – depending on the circumstances, this behaviour may constitute fraud

Falsification and manipulation of claims for work-related expenditure	
Use of the entity's funds for personal expenditure	Claiming employee expenses for business-related expenditure not incurred or incurred for personal use or benefit (supported by false or inflated receipts / invoices)
Double-dipping	Claiming multiple reimbursements for the same expenses or claiming for expenses paid personally using receipts for purchases already made via another of the entity's reimbursement systems

Diversion of incoming funds	
Accounts receivable fraud	Redirection of incoming receipts to a spurious account followed by write-off of accounts receivable balance
Unauthorised discounts	Processing unauthorised discounts for early payment of invoices where the discount value is fraudulently transferred to the employee's own bank account
An authorised application of unknown receipts	Funds can be received by an entity where the source of the funds is unknown and the funds are allocated to a suspense account pending rectification – a possible fraud involves the transfer of part of the balance of the suspense account to an employee's own benefit with a manipulation of the accounting system to conceal the theft
Inflating invoice value	Inflating the value of an invoice raised by the entity with receipts in payment of the invoice directed to a spurious account controlled by the staff member concerned who then redirects the correct (reduced) value of the invoice to the entity's correct account
Vendor overpayment	Deliberately overpay a vendor in payment of an invoice for goods or services validly received, claim a refund for the overpayment and then direct the remittance to a spurious bank account
Theft of cash all funds received	Fraudulently failing to record receipt of cash received and then misappropriate for own benefit

Payroll	
Timesheet fraud	Fraudulent submission of falsified timesheets for casual employees who did not work with diversion of resulting remuneration generated to own account
Fraudulent alteration of remuneration rates	Alteration of remuneration rates (salaries or hourly rates) in the payroll system in relation to the employee making the change or for another employee in exchange for personal benefit
Ghost employee fraud	Fabrication of fictitious employees on the payroll with remuneration paid to own account
Fraudulently failing to record personal leave	An employee taking personal leave (annual, long-service, sick or carer's leave) without recording the leave in the HR system
Worker's compensation fraud	Worker's compensation fraud – fraudulent claims for injuries not sustained

Assets and Inventory	
Asset theft	Theft of the entity's assets, including computers and other IT related assets
Information theft	Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans, etc)
Unauthorised private use of employer property	Use of employer property for personal use or benefit
Cash theft	Theft of petty cash

Manipulation of financial reporting	
Fraudulent manipulation of an entity's financial reporting	Fraudulent manipulation of financial reports in order to make it appear that a business entity has performed better (in financial or non-financial terms) than it has actually performed – this can be motivated by a need to demonstrate a certain level of personal performance in order to secure a performance bonus but may also be driven in the public sector by the need to meet political expectations

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

A5.4 Risk treatment tools

A5.4.1 SMART principle for co-designing fraud controls[17]

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

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

Specific	The control should have a clear and concise objective. They should also be well defined and clear to anyone with a basic knowledge of the work. Consider: who, what, where, when and why.
Measurable	The control and its progress should be measurable. Consider: • What does the completed control look like? • What are the benefits of the control and when they will be achieved? • The cost of the control (both financial and staffing resources).
Achievable	The control should be practical, reasonable and credible and should also consider the available resources. Consider: • Is the control achievable with available resources? • Does the control comply with policy and legislation?
Relevant	The control should be relevant to the risk. Consider: • Does the control modify the level of risk (through impacting the causes and consequences)? • Is the control compatible with the entity's objectives and priorities?
Timed	The control should specify timeframes for completion and when benefits are expected to be achieved.

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

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

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

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

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

The internal controls set out below can be used to:

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

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

Procurement and tendering
• Implement a tendering / contracting panel made up of independent personnel (i.e. unconnected to the procurement processes), to oversight the awarding of contracts
• Standard contract conditions and specifications to be used with variations to be approved by senior management
• Use evaluation criteria as agreed by the contract panel prior to tendering
• Contract terms and conditions should be those of the purchasing department and not subject to change without the written approval of senior management
• Clear audit trails with written records including formal authorisation of changes to original documentation
• Independent post-transactional review of a substantial sample of tendering and contracting transactions with a particular focus on high-risk transaction types
• Splitting of contacts should not be permitted unless authorised by senior management
• Management reviews of the reasonableness and competitiveness of prices
• Ensure contractors with a poor performance record are removed from the approved supplier's list

Falsification and manipulation of claims for work-related expenditure
• Limit the number of entity issued purchasing cards and users
• Set account limits with purchasing card providers (value, items that can be purchased etc.)
• Require employees with entity issued purchasing cards to submit itemised, original receipts for all purchases followed by lodgement of hard copy supporting documentation
• Independent rigorous examination of credit card transactions each month including detailed review of relevant receipts, invoices and other supporting documentation

Falsification and manipulation of claims for work-related expenditure
• Periodic review of a sample of hardcopy supporting documentation
• Monitor the entity's financial activity, compare actual to budgeted revenues and expenses
• Require an explanation of significant variations from budget

Diversion of incoming receipts
• Send official notification to all regular providers / suppliers with particulars of the entity's bank account with statement that this is the only account to which refunds should be remitted
• Independent post-transactional view of a sample of invoices rendered to identify any manipulations
• Independent post-transactional review of emails between accounts payable / accounts receivable personnel within the entity and customers / clients to determine if there is any indication of manipulation of invoices raised or payments made

Payroll
• Payroll system procedures and training
• Segregation of duties preventing payroll batch file payments or payroll master file changes without two approvers
• Limited system administrator access to the payroll system
• System controls to prevent changes to pay rates or salaries without approval
• Changes to payroll masterfile (e.g. particularly for bank account numbers) only available to employees via an HR 'kiosk' in the HR system – system unable to process a change of bank account number outside of the HR kiosk
• HR system to automatically generate a confirmation email to the employee where there has been a change of masterful data
• Rigorous approval process for creation of new employees in the payroll system

Payroll
• Timely notification process from HR to Payroll of employees due to resign from the entity
• Periodic review of payroll system audit logs
• Management review of variance reports from previous payroll run to confirm reasons for significant differences
• Employee background checks for new hires with access to the payroll system – this should include criminal record screening and specific questions about any previous integrity concerns / disciplinary findings etc.
• Mandatory password changes for those with access to the payroll system to a suitable strength and complexity
• Physical security of computers used by payroll staff with direct system access
• Electronic timesheet systems and approval process for overtime

Assets and inventory
• Physical security of desirable assets (i.e. laptops, IT equipment)
• Password protection and remote wiping capability in the case a laptop is lost or stolen
• Regular stocktakes of assets and inventory and updating asset registers
• Security of cash (i.e. petty cash) and gift vouchers in locked tins or a safe
• Tracking systems for assets and approval process for transfer of location
• Maintain vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the employee using the vehicle

Manipulation of financial reporting
• Active engagement with entity's external auditor in relation to the annual audit (i.e. working collaboratively with the auditor to identify any manipulation of the financial reporting)
• Analysis to identify unusual activity
• Detailed review of journal and other adjustments to the general Ledger with a focus, as a minimum, on high value transactions

Cyber-borne attack
• BitLocker protection of all IT assets to ensure security of data
• Access to databases/systems require unique user logon identification and password authentication
• Document authorisation that is needed to establish accountability and issue, alter, or revoke user access
• Prohibit shared user logon IDs and passwords, and user logon IDs and passwords
• Set database user access permissions that are based on the principles of privilege and separation of duties
• Restrict access to servers and office locations which contain sensitive and confidential data by physical security to authorised personnel
• Access to databases/systems require unique user logon identification and password authentication

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2021-22 reports

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

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia

9.1.1 2021/2022 Interim Audit Management Report

Attachment

SHIRE OF YILGARN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2022

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

INDEX OF FINDINGS	RATING		
Prior Year Issues	**Significant**	**Moderate**	**Minor**
1. Lack of supporting quotes for expenditure		✓	
2. Purchase orders dated after the invoice date			✓

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. A significant rating could indicate the need for a modified audit opinion in the current year, or in a subsequent reporting period if not addressed. However even if the issue is not likely to impact the audit opinion, it should be addressed promptly.

Moderate - 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 YILGARN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2022

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

Prior Year Issues

1. Lack of supporting quotes for expenditure

2022 Update
During the expenditure payments testing, it was noted that the required number of quotes was not obtained on 11 occasions out of the sample of 45 payments tested.

2021 Finding
During the expenditure payments testing, it was noted that the required number of quotes was not obtained on 1 occasion out of the sample of 50 payments tested.

2020 Finding
The Council's purchasing policy states that quotes are to be obtained in accordance with the following purchasing threshold bands:

Amount of Purchases	Form of Quotation (Minimum Requirements)
Up to $10,000	Direct Purchase, evidence of pricing to be recorded as an attachment to the Purchase Order
$10,001 - $50,000	Obtain at least one written quote
$50,001 - $100,000	Obtain at least two written quotes
$100,001 - $249,999	Obtain at least three written quotes

During the expenditure payments testing, it was noted that the required number of quotes was not obtained on 1 occasion out of the sample of payments tested.

Rating: Moderate (2021: Moderate)

Implication
The Shire has not adhered to the purchasing policy and as a result may commit to expenditure which has not been appropriately sourced by management representing value for money and quality as specified in the purchasing policy.

Recommendation
For purchases below the tender threshold, quotes should be obtained, in accordance with the Council's purchasing policy.
If instances arise where it is impractical to obtain the requisite number of quotations, the reasons should be recorded and attached to the purchase order at the time of the purchase being made.

Management's comments
After discussions with Butler Settineri, management acknowledges concerns that some purchases under $10,000.00 have not been undertaken in strict accordance with Council Policy. In response, all staff with authority to issue purchase orders have been advised, where a verbal quote has been obtained, a comment is to be included on the Purchase Order detailing the particulars of the quote, including from who the quote was received, for all purchases under $10,000 in order to comply with Council Policy. Executive staff will also commence a review of the Shire's Tendering and Purchasing Policy to determine if there are any further improvements or controls that can be implemented.

Responsible Person: Chief Executive Office, Executive Manager Corporate Services
Completion Date: 17 June 2022

SHIRE OF YILGARN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2022

FINDINGS IDENTIFIED DURING THE INTERIM AUDIT

2. Purchase orders dated after the invoice date

2022 Update
From our payments testing, we noted that 1 purchase orders out of a sample of 45 purchase orders tested were dated after the date of the suppliers' tax invoice.

2021 Finding
From our payments testing, we noted that 1 purchase orders out of a sample of 50 purchase orders tested were dated after the date of the suppliers' tax invoice.

Rating: Minor (2021: Minor)

Implication
There is no documented evidence that the ordering of goods was approved prior to ordering.

Management has not adhered to the Purchasing Policy and as a result may commit to expenditure which has not been appropriately authorised and may not represent valid business-related expenditure of the Council. This may potentially result in financial loss to the Council.

Recommendation
Management should ensure that purchase orders are obtained prior to the purchase of goods and services as required per the Purchasing Policy and that the purchase order number be referenced on receipt of the supplier's tax invoice.

Management's comments
Management will continue to enforce best practice principles in order to stop purchases happening outside of sequence.

All staff with authority to issue purchase orders have been advised in writing of their responsibilities in regards to purchasing and the production of a purchase order prior to ordering.

Finance team members have commenced and will continue to actively monitor for compliance.

Responsible Person: Chief Executive Officer, Executive Manager Corporate Services
Completion Date: 17 June 2022