Fraud risk management

Report 6: 2017–18

www.qao.qld.gov.au LinkedIn: Queensland Audit Office February 2018

Contact details

The Performance Audit Division of the Queensland Audit Office is the custodian of this report.

All comments and enquiries should be directed to:

Location	Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box	15396, City East Qld 4002
Telephone	(07) 3149 6000
Email	qao@qao.qld.gov.au
Online	www.qao.qld.gov.au

Copyright

Front cover image is an edited photograph of Queensland Parliament, taken by QAO.

ISSN 1834-1128.

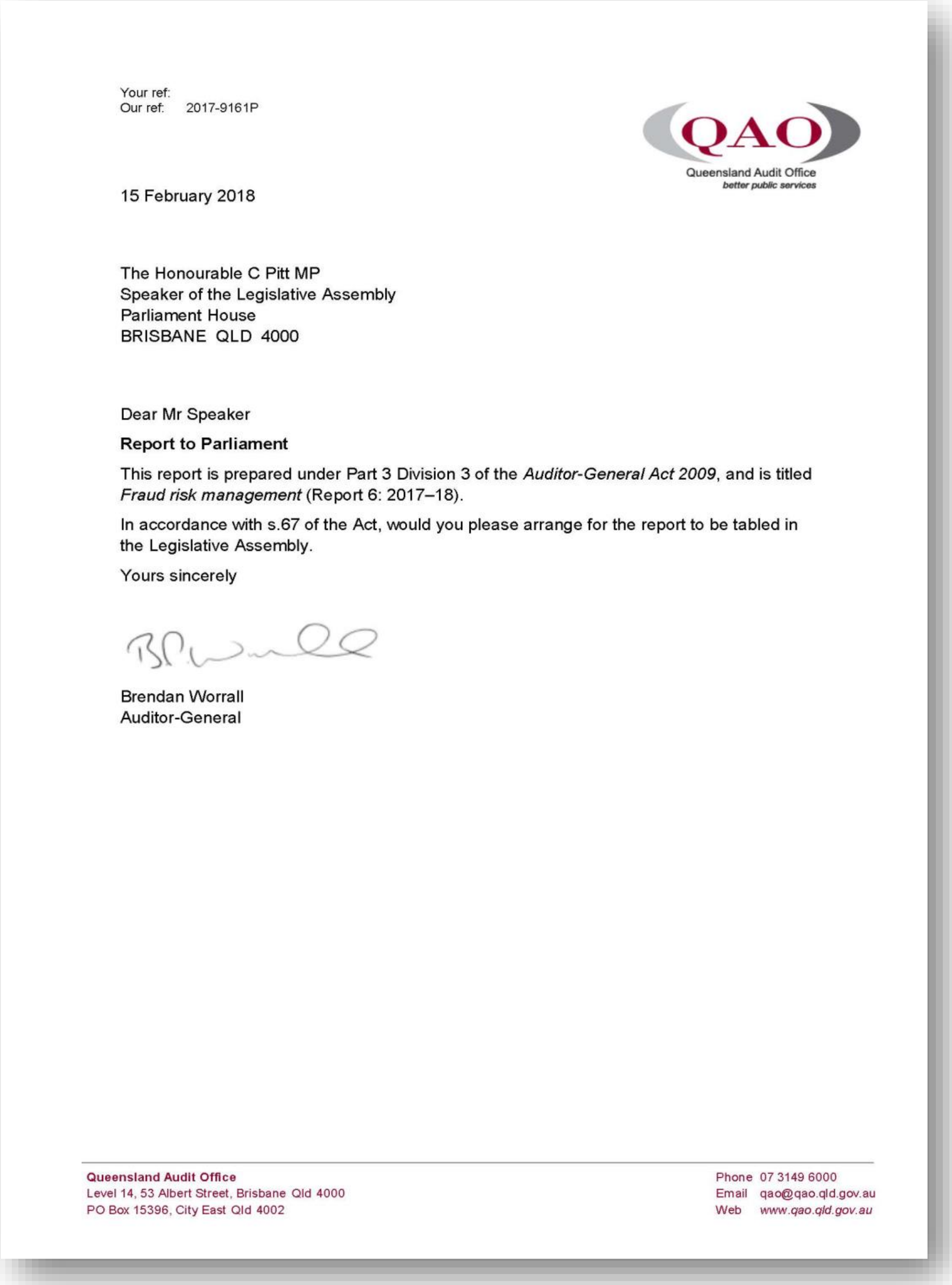
Reference to comments

In accordance with section 64 of the *Auditor-General Act 2009,* we provided a copy of this report to the Queensland Police Service, Public Safety Business Agency, Queensland Rail, Queensland Building and Construction Commission and Queensland Fire and Emergency Services. In reaching our audit conclusions, we have considered their views and represented them to the extent we deemed relevant and warranted when preparing this report.

Responses were received from the Queensland Police Service, Public Safety Business Agency, Queensland Rail, Queensland Building and Construction Commission and Queensland Fire and Emergency Services. The responses are in Appendix A.

Report cost

This audit report cost $255 000 to produce.



Your ref:
Our ref: 2017-9161P

QAO
Queensland Audit Office
better public services

15 February 2018

The Honourable C Pitt MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled *Fraud risk management* (Report 6: 2017–18).

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Brendan Worrall
Auditor-General

Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web *www.qao.qld.gov.au*

Contents

KEY FACTS

40 per cent of frauds in Australia take place over a five-year period before being discovered.*

Between April 2016 and September 2016, more than half of Australia's total fraud was reported in Queensland.*

In 2016–17, Queensland's Crime and Corruption Commission received 7 898 allegations of corruption (up 14 per cent since 2014–15).**

43 per cent of economic crime committed in Australian public sector organisations were identified because of tip-offs, whistleblowing or by accident.***

*Source: *KPMG (January 2017): Fraud barometer–A snapshot of fraud in Australia, April 2016 – September 2016.*

*Source: **Queensland Crime and Corruption Commission (September 2017): Effectiveness of Queensland public sector corruption risk assessments.*

*Source: ***PWC (2016): Global economic crime survey–Fighting fraud in the public sector IV.*

Audit objective and scope

In this audit we assessed if agencies appropriately identify and assess fraud risks, and apply appropriate risk treatments and control activities to adequately manage their exposure to fraud risks.

We assessed if the agencies' risk management plans effectively targeted and addressed fraud risks and if there were any obvious omissions from risk registers.

Our audit included five agencies:

- Public Safety Business Agency
- Queensland Police Service
- Queensland Fire and Emergency Services
- Queensland Rail
- Queensland Building and Construction Commission.

Summary

Introduction

Recent fraud attempts in the Queensland public sector highlight the need for agencies to implement effective fraud control measures.

In 2015–16:

- the Crime and Corruption Commission laid charges in 16 cases for fraud offences and recommended disciplinary action in a further 14 cases
- nine of Queensland's local government councils were targeted in a fraud scheme, resulting in $744 000 worth of fraudulent payments.

To effectively manage and identify fraud risks, an agency needs to examine its business environment to understand its potential exposure to fraud. Agencies that do not dedicate sufficient time and resources to understanding their fraud risks can be exposed without realising it. As a result, they may over or under control their fraud risks, investing too much or too little in fraud risk management.

Fraud and corruption are commonly associated, but they are distinct from one another. With reference to the Crime and Corruption Commission's *Fraud and corruption control: guidelines for best practice* (2005)

> Fraud is normally characterised by some form of deliberate deception to facilitate or conceal the misappropriation of assets, whereas corruption involves a breach of trust in the performance of official duties.

Legislation requires agencies to implement risk management systems to mitigate the risk of unacceptable losses, and to manage those risks that impede the agency's ability to deliver government services. Agencies should integrate fraud risk management within their agency's enterprise risk management approach.

Multiple sources provide guidance on better practice in fraud risk management:

- Crime and Corruption Commission's *Fraud and corruption control: guidelines for best practice*
- Queensland Treasury financial accountability handbook—*Fraud control*
- *Australian Fraud and Corruption Control* standard.

This is the third report QAO has completed on fraud risk management. The previous two covered departments and local government councils.

We developed a fraud risk assessment tool to provide agencies with a methodology to follow when assessing their inherent fraud risks (risks that exist before considering controls or mitigating factors). We used this tool to identify inherent fraud risks for the five agencies we audited.

Audit conclusion

None of the agencies we audited is effectively managing fraud risk, leaving themselves potentially exposed to fraud. Agencies have not applied the findings from our previous two reports on fraud risk management. We are still observing gaps in governance, fraud identification, detection, and prevention.

It is particularly concerning that agencies are not taking the opportunity to proactively manage fraud risk as the incidents and attempts of fraud become more prevalent and sophisticated.

While each agency has established a system and processes for enterprise risk management, none has effectively integrated fraud risk assessments into its existing practices. The audited agencies consider fraud risk on an ad hoc basis, if at all, and only assess it at a high level rather than through detailed analysis.

Although agencies have included some elements of better practice in their fraud and corruption control policies and plans, we still identified some gaps and opportunities to improve. In particular, agencies have not targeted their fraud and corruption control programs to the areas of greatest risk. Therefore, their plans for controlling fraud and corruption risks could be ineffective, particularly given that perpetrators of fraud are becoming more sophisticated in their approach.

Executives and senior managers state their commitment to fraud risk management in their policies, but they need to show their commitment by making sure their fraud and corruption control plans are implemented and monitored. They need access to better information from their staff to know what fraud risks are emerging and whether their controls to prevent fraud are working.

Summary of audit findings

Please note this is a summary of the audit findings. More information is in the following chapters.

Leading and developing a fraud risk management culture

Three of the five agencies' fraud policies state that senior management is committed to managing fraud risks, but this commitment is not evident in practice. While four agencies broadly state their approach to fraud risk management in their fraud policies and/or plans, none of the agencies could provide evidence of how they were applying it. This demonstrates a lack of commitment to implementing the approach the agencies outline in their policies and plans.

Each agency claims to have a zero tolerance (level of risk an agency can accept) to fraud and corruption. Only one agency articulates this in its risk appetite statement (outlines the amount of risk that an agency is prepared to accept or be exposed to at any point in time to achieve its objectives).

Establishing a fraud risk management framework

Fraud and corruption control policy

Most of the audited agencies have established a fraud and corruption control policy which contains better practice elements from the Crime and Corruption Commission's guidelines. However, agencies do not outline their approach for conducting fraud risk assessments, or identify what factors could influence fraud and corruption risks in their agency.

Of the four agencies with a fraud and corruption control policy in place, three of these were overdue for review at the time of the audit. These agencies have since developed a new draft of their policy, and one has since approved and published its new policy on their intranet.

Fraud and corruption control plan

Four agencies have a fraud and corruption control plan, but their plans do not include current or planned anti-fraud or anti-corruption activities. The plans demonstrate that agencies have not conducted a preliminary assessment of the agency's exposure to fraud risk to inform their fraud and corruption control programs. At the time of the audit, only one agency had an up to date fraud and corruption control plan in place. Three agencies' plans were overdue for review, and one agency did not have a fraud and corruption control plan. Three of the agencies with plans overdue for review have since developed a new draft of their plan, and one has recently approved and published a new fraud and corruption control plan.

Identifying and responding to fraud risks

Identifying fraud risks

Each audited agency conducts an annual risk management assessment for strategic and operational risks. However, none of the agencies specifically assesses the business environment for current and emerging fraud risk factors. This involves identifying business areas or service lines highly exposed to fraud risk to inform a detailed fraud risk assessment. As a result, they are not targeting their fraud and corruption control plans to emerging risks, or to areas of their operations with the greatest exposure to fraud risk.

None of the audited agencies provides its staff with training on identifying, mitigating, and managing fraud risks. There are no processes in place to scan for emerging fraud risks, and fraud risks do not feature in team discussions, even during the annual assessment of enterprise risks.

Responding to fraud risks

The audited agencies have not effectively integrated fraud risk management with their annual enterprise risk management activities. Although most audited agencies maintain strategic and operational risk registers, only one agency includes a fraud risk category. None of the other agencies has a fraud risk register, or includes a fraud risk category in their operational risk registers. The agency using a fraud risk category did not identify those fraud risks by undertaking a fraud risk assessment. Two other agencies each raised a single fraud risk but had not performed a fraud risk assessment to inform and justify the risks identified.

We assessed the adequacy of controls and risk treatments for agency-identified fraud risks. For those agencies that did not nominate fraud risks, we reviewed their risk registers and selected a sample of risks that had characteristics similar with fraud risks.

We observed that:

- while all audited agencies have risk owners, only two agencies have assigned control owners and established processes for them to assess and record the operational effectiveness of controls
- the wording of controls and risk treatments is generic. When using non-descriptive words, it is difficult to assign measures to assess the effectiveness of controls or risk treatments. A precise description helps to specify how the control or treatment would mitigate the risk.

Monitoring and reporting fraud risks

Senior management at each agency has limited visibility of its agency's potential exposure to fraud. They receive limited assurance over how well their controls and risk treatments mitigate fraud risks.

We observed that the audited agencies’ senior management teams monitor and report their enterprise risks, but there was no evidence this included fraud risks. Those agencies that identified fraud risks may assess these as part of their risk management processes. However, agencies do not have processes in place that are specifically targeted to assess, monitor and review their fraud risks, and conclude if actions to address them are effective. Senior management is not supported with adequate data and information to help it determine their agency's exposure to fraud risk and whether their fraud and corruption control plan is being implemented effectively.

We found evidence that the audited agencies’ governance forums discussed fraud incidents that have occurred, but there was no evidence they discussed current and emerging fraud risks. This indicates a reactive rather than proactive approach to fraud risk management.

Recommendations

We recommend that all public sector agencies:

1. self-assess against the better practices listed in this report to improve fraud control polices and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.
2. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks.

   The integrated framework should include the requirement to:

   - conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks
   - record fraud risks in a fraud risk register or using a fraud risk category in existing registers
   - train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks
   - ensure control owners regularly assess and report on the operational effectiveness of fraud controls
   - document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.
3. monitor through their governance forums, their agencies' exposure to fraud risk and the effectiveness of their internal controls to mitigate any risks.

   Key governance committees, including boards and audit and risk committees should:

   - review whether the agency has a comprehensive enterprise risk management framework in place, to effectively identify and manage risks, including fraud risks
   - ensure the agency has appropriate processes or systems to capture and assess fraud risks
   - review reports on fraud risks, and fraud incidents (that occur both within the agency and the broader public sector), considering how reported allegations and confirmed incidents may change identified fraud risks.

1. Context

This chapter provides the background to the audit and the context relevant to the audit findings and conclusions.

Fraud in the public sector

Fraud continues to be a significant risk facing the public sector. KPMG's latest fraud barometer (April–September 2016) reported that fraud in Australia increased since its previous report (October 2015–March 2016) from 116 to 143 cases, or from a total value of $381.1 million to $442 million. The KPMG document states that government agencies in Australia are the second highest category of victims to fraud: they lost $94.5 million over the reported period.

In 2015–16:

- the Crime and Corruption Commission laid charges in 16 cases for fraud offences and recommended disciplinary action in a further 14 cases
- nine of Queensland's local government councils were targeted in a fraud scheme, resulting in $744 000 worth of fraudulent payments.

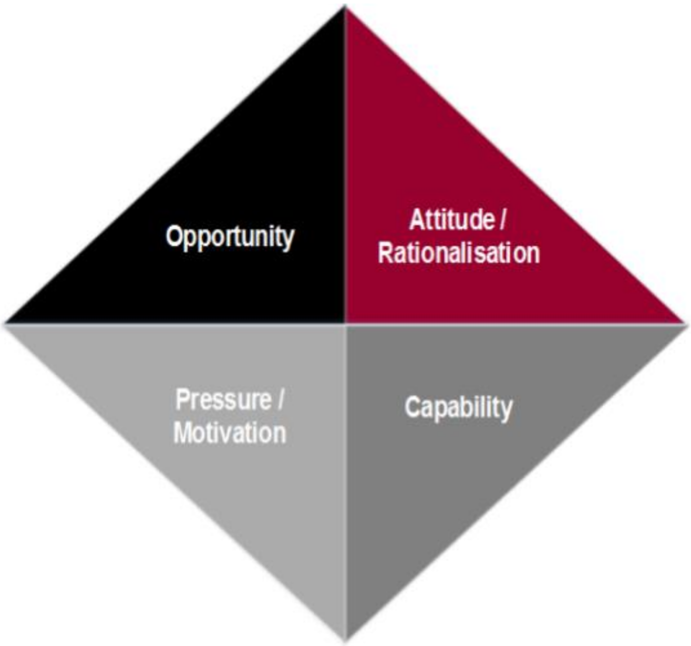
Public sector agencies are under increased pressure as government budgets continue to tighten, and available resources are restricted. The increasing expectation on agencies to do more with less presents conditions that are conducive for committing fraud.

It is generally accepted that various elements are required to work simultaneously for fraud to occur:

- pressure or incentive—a person can become motivated to commit fraud through pressure, which can be driven by a financial need or personal factors
- opportunity—can result from weak system controls, poor governance/management oversight, or misuse of position or authority
- rationalisation—where the person justifies in their own mind why their unethical behaviour is acceptable
- capability—characteristics and personality traits that help the person to exploit a foreseeable opportunity and execute fraud.

Figure 1A shows the fraud diamond which includes these four elements.

Figure 1A
Fraud diamond—four elements of fraud



Source: Queensland Audit Office adapted from The Fraud Diamond: Considering the Four Elements of Fraud, David T Wolfe and Dana Hermanson (2004).

Defining fraud

Fraud represents a deliberate deception to misappropriate assets or misuse information. It can cause significant disruption to an entity's operations, and significant financial loss. Section 408C of Queensland's *Criminal Code Act 1899* outlines fraud to be where a person dishonestly:

- applies property belonging to another, to their use or the use of another person
- obtains property from another
- induces a person to deliver property to another
- gains a benefit or advantage
- causes detriment
- induces a person to act in a way they can refuse, or abstain from acting in a way that they are entitled to act in
- takes property without making payment, knowing that payment is due.

Fraud is one example of corrupt conduct under the *Crime and Corruption Act 2001* (the Act). Under the Act, corrupt conduct is when a person performs their functions or exercises powers of their appointment in a way that:

- is dishonest or lacks impartiality
- involves a breach of trust either knowingly or recklessly
- involves a misuse of officially obtained information.

The focus of this audit was on fraud. Recently, the Crime and Corruption Commission issued a report on the *Effectiveness of Queensland public sector corruption risk assessments*. It assessed the corruption risk assessment processes for six agencies.

Previous reports to parliament

In March 2013, we reported to parliament on fraud risk management in Queensland public sector agencies. That report highlighted that the risk of fraud occurring and going undetected was unacceptably high.

In that report we recommended that:

- all public sector agencies assess their fraud control programs against the better practice principles highlighted in our report and, as required, implement a plan to address deficiencies highlighted by this self-assessment
- where the following are not in place, agencies should
  - conduct and regularly update their fraud risk assessments
  - implement routine data analytics over areas identified as inherently susceptible to fraud
  - use their fraud data to inform ongoing development of fraud control programs.

In June 2015, we reported to parliament on fraud management in local government. That report highlighted that most councils were not effectively managing their fraud risks. Following that audit, we published on our website our fraud and corruption self-assessment tool. This tool helps public sector agencies identify areas where they can improve their fraud controls.

In this audit, we examine how effectively five public sector agencies identify and assess fraud risks. We assess whether they apply appropriate risk treatments and control activities to manage their exposure to fraud risks. Because our most recent performance audit on fraud included local councils, we excluded them from this audit. Instead, we selected a sample of departments and statutory bodies.

Enterprise risk management

Enterprise risk management provides a framework that supports risk management processes to identify, assess, respond and monitor risks. Identifying and managing risks can help public sector agencies to minimise loss and effectively deliver government services. Legislation requires each Queensland public sector agency to implement an appropriate system of risk management that reduces loss and manages risks to service delivery. Structuring a well-defined enterprise risk management framework can assist agencies to:

- understand their environment, including external factors that may impede their ability to deliver on objectives
- manage identified threats and risks to the agency
- identify opportunities for innovation and development.

The Risk management standard AS/NZS ISO 31000:2009 recognises that the first step in risk management is to establish the context of an agency's risk exposure. This approach is not solely for fraud risk, but relevant for all risk types. The standard recommends four areas to consider when establishing context. These include:

- external context—external environmental factors and stakeholder relationships
- organisational context—internal agency objectives and strategies
- task or activity context—agency functions and activities
- risk criteria—used to evaluate the significance of risk.

Those responsible for identifying risks should research all areas to gain a holistic understanding of all risks affecting their agency.

To manage risk effectively, agencies need to establish processes for:

- identifying risks, and assessing their likelihood and impact
- nominating mitigating controls and treatments
- ongoing monitoring and reassessment of risks.

Enterprise risk management should integrate with strategic and operational planning, and encompass all types of risk that may affect an agency. This includes fraud risks, which represent another category of risk.

Integrating fraud risk into risk management

All agencies are subject to fraud risks and it is impossible to eliminate them. However, implementing processes to assess and identify fraud risk, as well as appropriate risk treatments and controls, can reduce an agency's exposure to fraud. It can also reduce costs if fraud occurs. Agencies should not manage fraud risks in isolation from other risks. They should continue to assess, identify, manage and monitor fraud risks in the same way as other risks. Like other risks, fraud risks can exist at the strategic and operational level.

Figure 1B shows the key elements supporting an enterprise risk management framework. It demonstrates that assessing and managing fraud risks forms part of enterprise risk management.

Figure 1B
Managing fraud risks as part of enterprise risk management

Culture and leadership

Legislative requirements and better practice guidelines

Enterprise risk management process	Fraud risk management activities
Establishing the context	**Fraud and corruption control policy** Approach to managing fraud risks. Review at least every two years.
Identifying risks	**Fraud risk assessment—entity** Gather external information from industry sources and identify all possible inherent fraud risks that could impact the agency.
Analysing risks	**Developing criteria** Develop a risk matrix to assess likelihood and consequence of fraud risks, using assessment results to determine overall risk rating.
	Fraud and corruption control plan Summarise agency's anti-fraud strategies—current and planned.
	Fraud risk assessment—detailed Detailed analysis of identified possible inherent fraud risks using developed criteria. Assess the likelihood, consequence and impact of each risk.
Documenting controls	**Controls/treatments** Identify current controls, and assess adequacy to mitigate fraud risk. Implement treatment if controls are inadequate.
Treating risk	
Monitoring and reporting	**Monitoring and reporting fraud risks** Record all fraud risks. Report on effectiveness of risk mitigation.

Source: Queensland Audit Office.

Leadership and culture

For risk management to be implemented effectively, it needs to be driven by an accountable officer, and fully supported by senior management. Both management and the accountable officer need to demonstrate their commitment to implement an effective program, and to be seen by their employees to support risk policies and procedures in a practical way.

A vital component of the enterprise risk management framework is fraud risk management. The framework will only be effective if senior management provides direction and generates a strong awareness for fraud risk management, while establishing the agency's tolerance for fraud. Senior management plays an important role in encouraging and supporting employees to identify and raise potential fraud risks. This approach creates a culture where employees feel confident to raise potential fraud activity or weaknesses in fraud control. Employees are the first line of defence, so it is important to ensure they know how to identify and report fraud risks.

A top-down and bottom-up approach is critical to effectively implementing a fraud risk management framework. It requires commitment from senior management to establish a strong culture that upholds high ethical standards, but also for operational areas to remain vigilant and committed to identifying and reporting potential fraud risks.

Legislative requirements and better practice guidelines

Requirements and guidance—risk management

Regular risk identification and analysis is a key element in an effective internal control structure. This includes fraud and corruption risks. Legislation, guidelines and standards are available to guide enterprise risk management.

Legislation

Section 61 of the *Financial Accountability Act 2009* requires that accountable officers and statutory bodies establish an appropriate system of risk management. Section 28 of the *Financial and Performance Management Standard 2009*, prescribes that agencies must provide for:

- mitigating the risk of unacceptable costs or losses associated with the operations of the department or statutory body to continue to provide government services
- managing the risks that may affect the ability of the department or statutory body to continue to provide government services.

Risk management standard

The Australian and New Zealand standard for risk management (Standard ISO 31000:2009 *Risk Management—Principles and guidelines*—AS/NZS ISO 31000) provides principles and generic guidelines on risk management. While no legislation mandates agencies to apply this standard, it helps agencies to integrate risk management into existing enterprise systems and link it to organisational objectives and culture. Effective application of the standard assists agencies to understand uncertainties that exist, and how best to manage these to deliver on strategic priorities.

Queensland Treasury risk management guidelines

In July 2011, Queensland Treasury issued *A Guide to Risk Management*. While the guide is not mandatory, it outlines minimum principles and procedures of a basic risk management process, and encourages better practice. The guide aims to help departments and statutory bodies adopt a consistent approach to risk management.

Requirements and guidance—fraud risk management

Queensland Treasury financial accountability handbook—fraud control

Queensland Treasury released an information sheet on fraud control, as part of its financial accountability handbook, last updating it in January 2017. The information sheet discusses early indicators of fraud, and effective processes for mitigating fraud risk. It recommends actions agencies should take to have effective approaches to addressing fraud risk that include:

- conducting robust risk assessments
- providing fraud awareness training to staff
- developing fraud policies and plans that target fraud risks specific to the agency.

The guidance also provides advice on agency and employee responsibilities when responding to a detected or suspected fraud.

Australian Fraud and Corruption Control standard

In March 2008, Standards Australia published the Fraud and Corruption Control standard (AS 8001-2008). The standard suggests an approach for controlling fraud and corruption. It takes a holistic approach to fraud and corruption control, focusing on:

- planning and resourcing
- prevention
- detection
- response.

The Crime and Corruption Commission 10-element model

The Crime and Corruption Commission (CCC) promotes an integrated and holistic organisational approach to effectively managing fraud and corruption. The commission developed a 10-element model in 2005, as part of better practice guidelines for managing fraud and corruption. The commission is currently updating the guidelines. To implement the model effectively, agencies must take a holistic approach to fraud and corruption, have full support from senior management, and must clearly communicate the model throughout the agency to ensure staff are aware of the model and how to implement it.

The 10 elements of the model include:

- agency-wide integrated policy—consists of coordinated and integrated instruments, mechanisms, arrangements and tools that assist with fraud and corruption control
- risk assessment—provides for mitigating the risk to the agency from unacceptable costs or losses associated with its operations, and managing the risks that may affect the agency's ability to deliver on government services. A risk management system is a requirement of the Financial and Performance Management Standard
- internal controls—first line of defence. While it cannot guarantee there is no error or fraud, it can reduce the risk of error and fraud occurring in the first place, and can help to detect fraud or error where it has occurred
- internal reporting—provides a location for people to report suspicious actions and suspected incidents of wrongdoing. It can help reduce the incidence of fraud and corruption, by identifying areas of risk and required system improvements
- public interest disclosures—measures taken to support parties involved and protect them against any form of reprisal that might result from reporting any form of wrongdoing
- external reporting—reporting mechanism in place to make the appropriate external integrity agencies aware of all suspected fraud and misconduct
- investigations—procedures undertaken in response to identifying suspected fraud or corruption, with the extent of the investigation depending on the seriousness of the allegation
- code of conduct—helps develop expectations and standards of behaviour within an organisation. It provides a framework within which employees perform their duties
- staff education and awareness—internalising ethical values and a commitment to accountability so that fraud and corruption prevention becomes inherent to the organisation
- client and community awareness—means a wide-ranging knowledge and understanding of the organisation's standards of corporate and employee behaviour, including everything from policies to codes of conduct.

The fraud and corruption control model represents better practice and provides agencies with self-evaluation checklists they can use to assess how adequate their systems and processes are against each element.

While Queensland Treasury's guide and the CCC's model provide guidance, agencies should tailor their approach to risk management to suit the nature and operations of their businesses. A clear and well-structured framework and strong governance structure will help to support compliance with risk management principles and effective risk management practices.

Implementing fraud risk management

In this audit we refer to better practices in preventing, detecting and responding to fraud risks. We have defined better practice elements of fraud risk management based on the guidance available to public sector entities as noted above.

We assessed the effectiveness of the five public sector agencies within the scope of this audit in identifying, assessing and managing fraud risks, by comparing them to the better practice elements.

Figure 1C shows the elements of better practice fraud risk management.

Figure 1C
Elements of better practice fraud risk management

Element of fraud risk management	Description
Fraud and corruption control policy	▪ outlines approach to fraud risk management and how to apply it ▪ communicates senior management's commitment to managing fraud risks, and the agency's values and business practices ▪ links with enterprise risk management principles ▪ identifies fraud risk factors that can lead to fraud and corruption ▪ references related legislative requirements and guidelines ▪ outlines employee roles and responsibilities ▪ includes policy date and document review date.
Fraud risk assessment—entity	▪ high-level entity assessment identifies business units and service areas that are most inherently susceptible to fraud risks ▪ assesses the business environment, agency strategies, external factors, threats and opportunities that may increase the agency's exposure to fraud risks.
Fraud and corruption control plan	▪ records agency-specific fraud and corruption risks ▪ outlines agency anti-fraud and anti-corruption strategies to mitigate risks, outlining current and planned activities ▪ assigns responsibility and implementation dates for strategies ▪ supported by monitoring procedures to measure the effectiveness of mitigating strategies, and to hold employees accountable for assigned controls and treatments ▪ complements the fraud and corruption control policy.
Fraud risk assessment—detailed	▪ uses results of a high-level entity risk assessment to conduct a more detailed assessment that targets specific areas, most at risk of potential fraud exposure ▪ identifies fraud risks that specifically relate to an agency's business units and service areas ▪ produces a targeted response to identified fraud risks, considering feasibility, and measures costs against the benefits.
Fraud controls	▪ activities that prevent or detect errors to mitigate identified fraud risks ▪ detective controls are reactive, and assess completed transactions, with a view to correcting issues promptly ▪ preventative controls reduce the risk of fraud happening in the first place ▪ effective fraud controls balance the cost of operating them against the risk mitigation that they achieve ▪ should regularly review to ensure controls remain relevant, appropriate, and provide the most assurance. May also detect unnecessary or compensating controls.
Fraud treatments	▪ process of selecting and implementing actions to modify risk We can generally classify risk treatment or response as one of the following: ▪ accept ▪ reduce ▪ transfer ▪ avoid. Treatment plans should include: ▪ treatment or action ▪ risk owners ▪ review date ▪ means of reporting status ▪ suitable performance measures.

Element of fraud risk management	Description
Fraud risk monitoring and reporting	▪ internal systems and governance arrangements to regularly review existing fraud risks, and monitor/assess the effectiveness of fraud controls and treatments. Also to identify new and emerging fraud risks ▪ discuss the results of fraud risk monitoring and analysis ▪ keeps senior management informed of fraud risks that potentially expose the agency and provides assurance over the effectiveness of mitigating activities ▪ can present trends, common risks across the agency and wider public-sector issues that may have an impact ▪ helps inform management decisions.

Note: We referred to multiple sources for better practice guidance, including Crime and Corruption Commission's Fraud and Corruption Control: guidelines for better practice; Queensland Treasury's risk management guidelines and Financial Accountability Handbook, the Australian and New Zealand standard for risk management, the Australian Fraud and Corruption Control Standard and learnings for our report, Fraud Management in Local Government (Report No. 19: 2014–15).

Source: Queensland Audit Office.

Roles and responsibilities

The *Financial Accountability Act 2009* requires that all accountable officers and statutory bodies establish and maintain appropriate systems of internal control, including risk management. They need to manage all strategic and operational risks in accordance with their risk management system.

All public sector agencies and their employees are responsible for preventing, detecting and responding to fraud. Figure 1D shows key roles and responsibilities common to all agencies for fraud risk management.

Figure 1D
Key roles and responsibilities—fraud risk management

Role	Responsibilities
Accountable officer/ chief executive officer (CEO)	▪ demonstrates a strong commitment to fraud risk management ▪ articulates the agency's tolerance/appetite for fraud ▪ sets clear expectations for employee roles and responsibilities for managing fraud risks.
Executive/ senior leadership team	▪ actively supports fraud risk management ▪ endorses fraud and corruption control policy and plan ▪ oversees and reflects on potential fraud risk exposures.
Fraud and corruption control officer/risk team	▪ accountable for implementing and ongoing monitoring of the agency's program for fraud and corruption control ▪ regularly report to the accountable officer/CEO and senior management (including board) on actual and inherent fraud risk exposures ▪ develop and implement fraud policy, plan and related processes ▪ monitor and report on agency's risk environment and risk profile ▪ oversee agency's management of fraud risk, and implementation of risk management framework ▪ implement processes to hold risk and control owners accountable for managing risk and assessing controls.
Risk owners	▪ regularly assess allocated risks, and assess the operational effectiveness of controls and treatments ▪ document results of assessment and report to risk management team.
Control owners	▪ regularly test the operational effectiveness of assigned controls and mitigating activities ▪ meet implementation timeframes ▪ document and justify results of controls assessment.
Employees	▪ actively assess the agency and respective divisions for potential fraud risks, and record in risk registers ▪ report actual and suspected incidents of fraud ▪ display integrity and uphold code-of-conduct.

Source: Queensland Audit Office.

2. Managing fraud and corruption risk

We assessed whether the audited agencies have appropriate fraud risk management practices and conduct regular fraud risk assessments to identify potential and emerging fraud risks. In each section, we begin with a statement to show what better practice looks like.

Introduction

To effectively identify, prevent, detect and respond to fraud, agencies need to have a robust and comprehensive approach to fraud risk management. The approach needs to:

- clearly communicate a low tolerance for fraud and establish senior management's commitment to fraud risk management
- provide a clear direction on how an agency will mitigate fraud risk, supported by internal control processes and procedures
- include explicit guidance to show employees how to identify potential fraud risks and how to design and implement mitigating activities
- promote employee accountability for identifying and managing fraud risks
- establish detailed analysis and regular reporting of the agency's potential exposure to fraud risk.

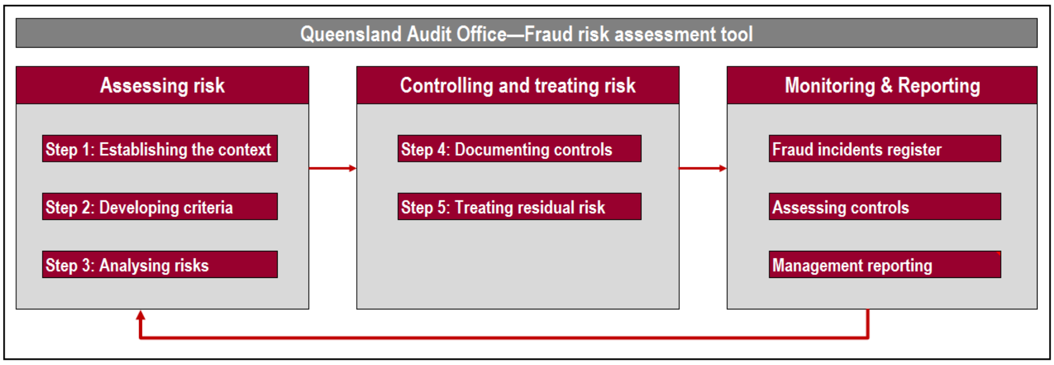
We examined how robust and comprehensive the selected agencies' approaches were to managing fraud and corruption risks.

As part of this audit we developed a fraud risk assessment tool to help public sector agencies document their assessments of fraud risk; how they will control fraud risks; and how they will monitor and report their fraud risks.

We applied the tool to each of the in-scope agencies, to assess and document potential inherent fraud risks, and provided these to the agencies we audited for their consideration. (Appendix C.)

Figure 2A provides a snapshot of the tool's structure, which agencies can follow to help them implement better practice fraud risk management within their existing enterprise risk management framework. It includes five steps for assessing, controlling and treating fraud risks.

Figure 2A
Fraud risk assessment tool



Queensland Audit Office—Fraud risk assessment tool

Assessing risk
- Step 1: Establishing the context
- Step 2: Developing criteria
- Step 3: Analysing risks

Controlling and treating risk
- Step 4: Documenting controls
- Step 5: Treating residual risk

Monitoring & Reporting
- Fraud incidents register
- Assessing controls
- Management reporting

Source: Queensland Audit Office.

Leading and developing a fraud risk management culture

Senior management's commitment to fraud risk management

To effectively implement policies and related procedures, an agency's accountable officer needs to drive its implementation, and set clear expectations for their employees in its fraud policy. The agency's fraud and corruption control policy should demonstrate senior management's commitment and clearly outline the roles and responsibilities of the agency's accountable officer, with respect to fraud risk management.

While most audited agencies' fraud policies and plans state senior management's commitment to managing fraud, it is not evident in practice. While four agencies outline their approach to fraud risk management (which includes conducting fraud risk assessments), none of the agencies provide evidence of how they are applying it. This demonstrates a lack of commitment to the agency's approach outlined in its policy and plan.

Only one agency specifies its tolerance for the treatment and escalation of fraud and corruption risk in its risk appetite statement. Not doing so makes it difficult for employees to understand management's expectations, and practically apply tolerance levels to risk assessments.

Of the five agencies we audited:

- four express a zero tolerance for fraud in their fraud policies and/or plans
- three articulate senior management's commitment to fraud risk management in their fraud policies and/or plans
- none demonstrate commitment to its approach to fraud risk management in its fraud policy and/or plan
- four do not specify their tolerance for the treatment and escalation of fraud risk in their risk appetite statements.

Most audited agencies state in their fraud risk governance documents that their accountable officer is primarily responsible for overseeing fraud risk. This provides a clear line of overall accountability, and demonstrates the accountable officer's support for fraud risk management. Employees are more inclined to comply with the policy and/or plan when the support from the accountable officer is explicit.

Of the five agencies we audited:

- Three agencies acknowledge in their fraud risk policy and/or plan that the accountable officer has primary responsibility for fraud risk.
- Two agencies do not articulate in their fraud risk policy and/or plan the accountable officer or senior management's commitment to fraud risk management.

Risk team and employee awareness

The agency should assign accountability for implementing and monitoring effective fraud risk management practices, and for developing employee awareness. Nominated officers should hold appropriate qualifications, skills and experience to fulfil the role.

Each agency has assigned responsibility for fraud risk management to officers within its agency. However, the teams are small and often have competing responsibilities across multiple areas. This can put a strain on a team's capacity to manage and provide guidance on fraud risks to employees across their agency.

In one agency, the team managing fraud risks sat within the internal audit unit. Combining risk and internal audit compromises the independence of internal audit to provide assurance to senior management on how effectively the agency identifies and manages fraud risks. During this audit, the agency moved the responsibility for managing fraud risks to a separate new risk management unit.

None of the audited agencies is increasing staff awareness or capability in fraud risk management by conducting training or awareness sessions. However, all five agencies are now taking steps to develop training materials on fraud risk management to increase staff awareness.

Of the five agencies audited:

- All agencies have nominated an individual and/or team responsible for fraud risk management.
- Two agencies provide online training for their employees on code of conduct and ethical decision-making, and another has presented risk workshops, but none focus on fraud risk management, or how to conduct a fraud risk assessment.

Establishing fraud risk management policies and processes

Fraud and corruption control policy

A fraud and corruption control policy should articulate the importance of fraud risk management, outline how the agency will apply it, advise whom it relates to, and establish clear lines of accountability.

The Crime and Corruption's *Fraud and Corruption Control: guidelines for best practice* (the CCC guidelines) advises agencies should review their fraud policy at least once every two years, ensuring it remains current and relevant to the agency.

There is no prescribed format for preparing a fraud and corruption control policy, but the CCC's guidelines list key elements that an agency should include. Most of the audited agencies have established a fraud and corruption control policy containing these better practice elements. There are some common omissions compared to better practice fraud policies. These include:

- communicating agency values and business practices
- outlining key influencing factors that lead to fraud risk
- clearly articulating senior management’s commitment to fraud risk management.

Of the five agencies we audited:

- two do not have a fraud and corruption control policy
  - one has a fraud and corruption control plan that covers some but not all better practice elements
- three have fraud and corruption control policies, but the versions available at the time of the audit were developed more than three years ago, and were overdue for review
  - three agencies were developing new drafts of new fraud and corruption control policies during our audit; one has since published its policy on its intranet
  - the draft versions contain most better practice elements we expected.

Figure 2B shows the results of our assessment for three of the agencies that had a fraud and corruption control policy.

Figure 2B
QAO assessment of fraud and corruption control policies against the CCC guidelines

CCC guideline key element	Findings
Clearly communicates the agency's values and business practices	Three agencies who have a fraud and corruption control policy have established a zero tolerance for fraud and made explicit statements about their commitment to reporting incidents of fraud, and adopting practices to detect, prevent and respond to fraud. However, none of these agencies communicate their values and business practices within their policy.
Articulates the Chief Executive Officer and senior management’s commitment to fraud risk management	Two agencies note the accountable officer has primary responsibility for fraud risk management, and express senior management's commitment. One agency does not state the accountable officer or senior management's commitment to fraud risk management.
Uses a risk management philosophy and references underlying legislation and/or guidelines	All three agencies reference related guidelines and legislation, acknowledging a risk-based approach to fraud control. One of these agencies does not define fraud in their policy, but defines the term in its fraud and corruption control plan.
Identifies key factors that influence fraud and corruption risk	None of the three agencies identify key influencing factors that might result in fraud and corruption risk.
Integrates related policies to control the incidence and impact of fraud risk	Each agency refers to related policies, plans and documents that support fraud risk management.
Outlines related responsibilities	Each agency outlines the responsibilities of key officers involved in fraud risk management.
Includes the date of the policy and anticipated review date	All policies include the date and the anticipated review date. All three were overdue for review at the time of the audit. The three agencies have since developed a new draft of their policy. One agency has approved and published the final version.
Accessible to employees	All policies are accessible on each agency's intranet.

Source: Queensland Audit Office based on our assessment of the audited agencies’ fraud and corruption control policies against the Crime and Corruption Commission’s Fraud and Corruption Control: guidelines for best practice.

Fraud and corruption control plan

The Australian Fraud and Corruption Control standard (AS 8001-2008) defines a fraud and corruption control plan as:

A document summarising an entity's anti-fraud and anti-corruption strategies.

The plan should contain fraud risks specific to the agency identified through fraud risk assessments. It should include the risks and the plans to mitigate them. The fraud risk assessments help to identify specific areas or functions in the agency most susceptible to fraud risk. This allows the agency to include actions in its fraud and corruption plan to develop mitigation strategies that specifically target these areas.

Most audited agencies have a fraud and corruption control plan. However, the fraud risks and strategies are not agency-specific or identified through a fraud risk assessment, for most agencies. By including generic fraud risks in the fraud and corruption control plan, agencies are not effectively targeting their inherent fraud risks. As a result, the ‘real’ fraud risks inherent to the agency may be under- or over-controlled. Mitigating actions will not be specific and may be difficult to measure.

Of the five agencies we audited:

- Four agencies have a fraud and corruption control plan.
- None of the agencies performs an entity-level fraud risk assessment to identify areas of greatest risk, to inform a more detailed analysis of agency fraud risks.
- Only one agency lists agency-specific fraud risks, but does not monitor or record these in risk registers. Other agencies only identify generic examples of fraud risks.

The Australian Fraud and Corruption Control standard, and the Commonwealth fraud control framework provide some guidance on developing a fraud and corruption control plan. They recommend that the plan should outline an agency's approach to managing fraud, include current and planned strategies to mitigate fraud, and establish a program to monitor the plan's implementation and ensure its regular review.

There are some common omissions compared to better practice fraud plans. These include:

- conducting an entity-level fraud risk assessment to identify business areas most at risk of fraud, to inform detailed fraud risk assessment
- describing anti-fraud and anti-corruption strategies to mitigate any identified fraud risks
- outlining current and planned activities to achieve outcomes of the plan
- listing controls and treatments for mitigating identified fraud risks.

Figure 2C shows the results of our assessment of the four agencies that have fraud and corruption control plans.

Figure 2C
QAO assessment of fraud and corruption control plans against better practice

Better practice guidance—key element	Findings
Current anti-fraud and anti-corruption strategies	All four agencies do not include details of current anti-fraud and anti-corruption strategies. While three out of the four agencies reference generic control strategies, grouped under categories like prevention, detection and response, these do not represent an actual program of activities that the agency is undertaking to address identified fraud risks.
Planned fraud control program and activities—identified through risk assessment	None of the four agencies: ▪ includes details of planned activities to achieve anti-fraud and anti-corruption strategies. One agency includes examples, but not actual planned activities ▪ performs an entity-level fraud risk assessment to inform their activities to mitigate identified fraud risks.
Treatment strategies or controls to mitigate identified fraud risks	Only one agency lists identified fraud risks and related controls, however these are out-of-date. The current fraud and corruption control plans for two out of the three remaining agencies list examples of fraud or possible situations that could lead to fraud, but these are generic and not based on a risk assessment specific to the agency. The third agency lists risks resulting from fraud and corruption, however these are generic, broad and representative of consequences, rather than specific fraud risks.
Regular review	At the time of the audit, only one out of the four agencies had a current fraud and corruption control plan in place. The other three agencies were using plans that were overdue for review. The three agencies have since developed a new draft and one has approved and published its plan. All plans nominate a document review date or period.
Assigns responsibility to officers for implementing strategies, including timeframes	None of the four agencies assigns employees with responsibility for implementing specific strategies, or due dates for actions.

Note: We referred to multiple sources for better practice guidance, including *Crime and Corruption Commission's Fraud and Corruption Control: guidelines for better practice*; Queensland Treasury's *Financial Accountability Handbook*; and the *Australian Fraud and Corruption Control Standard*.

Source: Queensland Audit Office based on our assessment of the audited agencies' fraud and corruption control plans against better practice.

Identifying and responding to fraud risks

Identifying fraud risks

The Australian Standard on fraud and corruption control (AS 8001:2009) recommends that entities conduct a comprehensive review of fraud and corruption risks every two years. The standard advises entities to consider not only the existing environment and current threats, but also those risks that are emerging.

Periodic fraud risk assessments are essential to identify, understand, document and mitigate fraud risks across all business levels and services. They help agencies to identify gaps or weaknesses in their internal control environment and to develop treatments to reduce the residual risk of fraud to a tolerable level.

Integrating fraud risk assessments within an agency's enterprise risk framework ensures that the agency can support the identified fraud risks with detailed analysis, and evidence.

All five agencies have established systems and processes for enterprise risk management, at various stages of maturity, to identify and manage risks. However, none of the agencies perform fraud risk assessments as part of their existing risk management procedures. While three agencies have raised a combined total of 10 fraud risks, the risks did not result from a comprehensive assessment of fraud risk. Fraud is a brief consideration for agencies at best, which they do not factor into a detailed assessment. Agencies do not specifically assess the business environment for current and emerging fraud risk factors to identify highly exposed areas that could inform a detailed fraud risk assessment.

Of the five agencies we assessed:

- None of the agencies conducts a preliminary assessment of entity-level fraud risks to determine which areas of their business they should conduct a more detailed fraud risk assessment on.
- None of the agencies conducts detailed fraud risk assessments, although four stated in their fraud policies and/or plans that employees should conduct a regular fraud risk assessment.
- None of the agencies provides step-by-step guidance to direct employees on how to undertake a fraud risk assessment.
- None of the agencies incorporates fraud risk assessments into its annual assessment of strategic and operational risks.
- All agencies are yet to formalise how they each identify and respond to fraud, and to integrate this within their enterprise risk management framework.
- One agency has raised several operational fraud risks, and another two agencies have raised one operational and one strategic fraud risk, respectively. None of these risks resulted from performing a fraud risk assessment.

Because none of the audited agencies were performing fraud risk assessments, this limits the agencies' ability to fully comprehend:

- potential fraud risks
- significance of inherent fraud risks
- an appropriate response to mitigate inherent fraud risks.

In the absence of this assessment, agencies are leaving themselves exposed. They will have limited ability to identify existing and emerging fraud risks, identify gaps in controls and develop appropriate treatments.

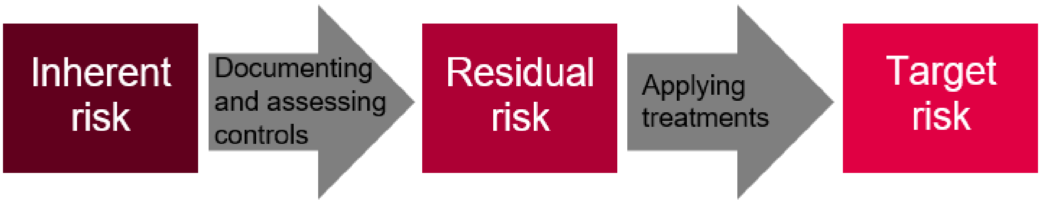
Responding to fraud risks

Documenting controls

Agencies should document their existing internal controls and link them to the inherent fraud risks identified in their fraud risk assessment. They can then assess their residual risk of fraud and determine the need for additional risk treatments.

When identifying fraud risks, agencies should first establish an inherent risk rating (combined assessment of risk likelihood and impact before controls) for each fraud risk they identify. Agencies should then identify, document and assess control activities they already have in place to mitigate the risk, and determine the extent of risk that remains (residual risk). If the residual risk rating exceeds the agency's tolerance for fraud risk, the agency needs to develop a treatment plan to reduce the risk rating within this tolerance level. This is the 'target risk' or level of risk, after applying treatments, that is tolerable for the agency. Figure 2D shows this process.

Figure 2D
Overview: controlling and treating fraud risks



Source: Queensland Audit Office.

In walkthroughs we conducted with risk owners at all five agencies, we found that they had relevant controls in place to mitigate some of the fraud risks we identified. However, none of the agencies maintain detailed descriptions of their internal controls in their risk registers. As a result, management and risk owners are not able to assess the appropriateness of the controls' design or test how effective the controls are at preventing or detecting fraud.

Of the five agencies we audited:

- Four out of the five agencies maintain strategic and operational risk registers.
- Four of the agencies do not have either a fraud risk register or include a fraud risk category to record fraud risks and related controls and treatments in their existing risk registers.
- Only one agency has established a fraud risk category for its operational risks.

Assessing controls

Agencies should periodically assess their internal controls to confirm their effectiveness and to confirm their residual risk ratings. Assessing controls should include:

- **meeting with control owners to identify gaps in the mitigating controls**
- **testing the controls to assess their implementation and effectiveness.**

We found that only two agencies nominate control owners, and implement a formal process where control owners provide assurance to risk owners over the operational effectiveness for their assigned controls. Without this assessment, agencies are limited in their ability to confirm the residual risk and identify if additional risk treatment is necessary.

Of the five agencies we audited:

- Each agency has assigned responsible officers to manage individual risks, but only two agencies have introduced control owners to provide assurance over the operational effectiveness of controls, and applied this to fraud risks.
- Both of the agencies with control owners require them to regularly document the outcome of their assessments in an agency risk management system or register.

We selected a sample of risks from each agency to assess their controls and risk treatments. Recognising that agencies do not conduct fraud risk assessments, we selected risks that had characteristics that were similar with fraud risks, or those that the agency had labelled as fraud risks. Only three agencies categorised some risks as fraud risks, despite not conducting a fraud risk assessment. We observed that control descriptions were generic, making it difficult to:

- understand how the control mitigates the risk
- assign an appropriate metric to measure the effectiveness of the control.

Of the five agencies we audited:

- All agencies nominate controls (mitigating strategies).
- Three agencies do not have processes in place for risk owners or senior management to obtain assurance over the operational effectiveness and relevance of controls.
- Control descriptions for all agencies are generic and lack detail to make it clear how the control would mitigate the risk. For some controls, we needed to drill down into the supporting documentation of related policies and procedures to better understand what the control was.

Applying treatments

Agencies should develop risk treatments for fraud risks that have a residual risk rating that exceeds the agency's tolerance for fraud risk. The treatment needs to reduce the risk rating to sit within its tolerance level (target risk). Agencies should document details of how they will implement their fraud risk treatments, which clearly define:

- **the allocation of responsibility for implementing the treatment**
- **timeframes for implementing and reviewing the treatment.**

Across the five agencies, risk treatments are either applied inconsistently or not at all. Descriptions do not adequately outline treatments and how they mitigate the related risk. The absence of formal processes and risk awareness among employees limits the effectiveness of risk treatments, and could potentially result in agencies ineffectively managing their potential exposure to fraud, and related risks. Uncertainty regarding treatments among employees indicates that there is benefit in providing more guidance and training to clarify when to develop and apply risk treatments.

Of the five agencies we audited:

- One agency does not apply risk treatments after controls, even if the risk has a medium to high residual risk rating.
- Treatment descriptions are generic and lack sufficient detail to articulate how the treatment will mitigate the risk.
- One agency applies risk treatments inconsistently, applying treatments to some but not all risks with a medium to high residual risk rating. However, the agency has also developed treatments for some risks with a low residual risk rating.
- Meetings with risk owners and employees confirmed that there was uncertainty about whether a treatment was necessary, and when to apply a treatment.

Monitoring and reporting fraud risks

Fraud risk analysis

Monitoring and analysing fraud risks and discussing the results in key governance committees is an important part of any robust approach to fraud risk management. It provides an opportunity for agencies to:

- **ensure that nominated controls and treatments are operating effectively**
- **assess if fraud risks are being over- or under-controlled**
- **identify emerging fraud risks**
- **understand an agency's potential fraud risk exposure.**

In all five agencies, boards and senior management do not receive information on potential fraud risks, areas of exposure, or whether controls and risk treatments were effective. Agencies have processes in place to monitor and report on risk management, but there is no evidence of specific analysis of fraud and corruption risks. This could leave senior management ill-informed about their agency’s potential exposure to fraud, the impact of external factors, and whether their agency is over- or under-controlling its fraud risks. Senior management is not supported with sufficient data to determine what their agency’s level of exposure is, or if its policy and plan are implemented effectively.

There is limited discussion in teams to determine emerging fraud risks, and no processes to detect emerging fraud risks in any of the agencies we assessed. Only one agency's finance team conducts some data analysis to scan for or record fraud risks across functional areas (business units).

There is limited data available across all five agencies to draw a conclusion about the operational effectiveness of controls or mitigating strategies for fraud risks. This is a symptom of agencies not capturing fraud risk information centrally or consistently and employees not raising fraud risks, or understanding how to undertake a fraud risk assessment.

If boards or senior management do not regularly receive information on fraud risks, or discuss those that relate to their agency, they cannot gain assurance or demonstrate that they objectively understand the level of their agency's potential fraud risk exposure.

We reviewed the minutes of key governance committees from each agency, including:

- board
- audit and risk committee
- other committees related to risk.

Of the five agencies we audited:

- All discuss enterprise risk management, including strategic risks in their governance committees.
- None of the governance committees we assessed discuss management of fraud risks.
- All agencies have a process to advise senior management on reported incidents and use their governance committees to discuss learnings.
- No agencies have established a process to discuss fraud risks or the agency’s potential exposure to fraud.
- Limited data is captured across all five agencies, to enable the responsible risk officer of each agency to report on the operational effectiveness of controls or mitigating strategies for fraud risks.

Monitoring and responding to internal fraud incidents

The Australian and New Zealand standard for risk management advises that senior management should have knowledge of the incidents of fraud and corruption in their entities in the last five years and how the entity dealt with the matters in terms of disciplinary action and internal control enhancement.

Agencies should reflect on fraud incidents they know of, to inform their fraud risk assessment and to develop and implement effective controls and treatments to mitigate similar frauds from occurring again.

Section 21 of the *Finance and Performance Management Standard 2009*, requires an accountable officer or a statutory body to record all losses they suspect result from an offence or corrupt conduct. The standard requires the agency to notify the following of incidents resulting in a material loss:

- an appropriate minister
- the Queensland Police Service or Crime and Corruption Commission
- the auditor-general.

To comply with legislation, agencies should maintain internal reporting mechanisms to record all losses resulting from suspected fraud and/or corrupt conduct. Agencies should reflect on the details of fraud incidents, internal and external to the agency, and consider contributing factors when conducting fraud risk assessments. This can help inform potential fraud exposures that may be relevant to the agency, and help the agency to develop some learnings that may lead to the tightening of internal controls and risk treatments.

Although the five agencies we audited record fraud incidents, they do not have a standardised mechanism for recording and incorporating them into inherent fraud risk assessments and internal control assessments.

In our fraud risk assessment tool, we have included a register for capturing the details of an agency's fraud incidents and its responses. By maintaining a register of fraud incidents, agencies can link incidents of fraud to an existing fraud risk, or create a new risk where there is a gap.

Appendices

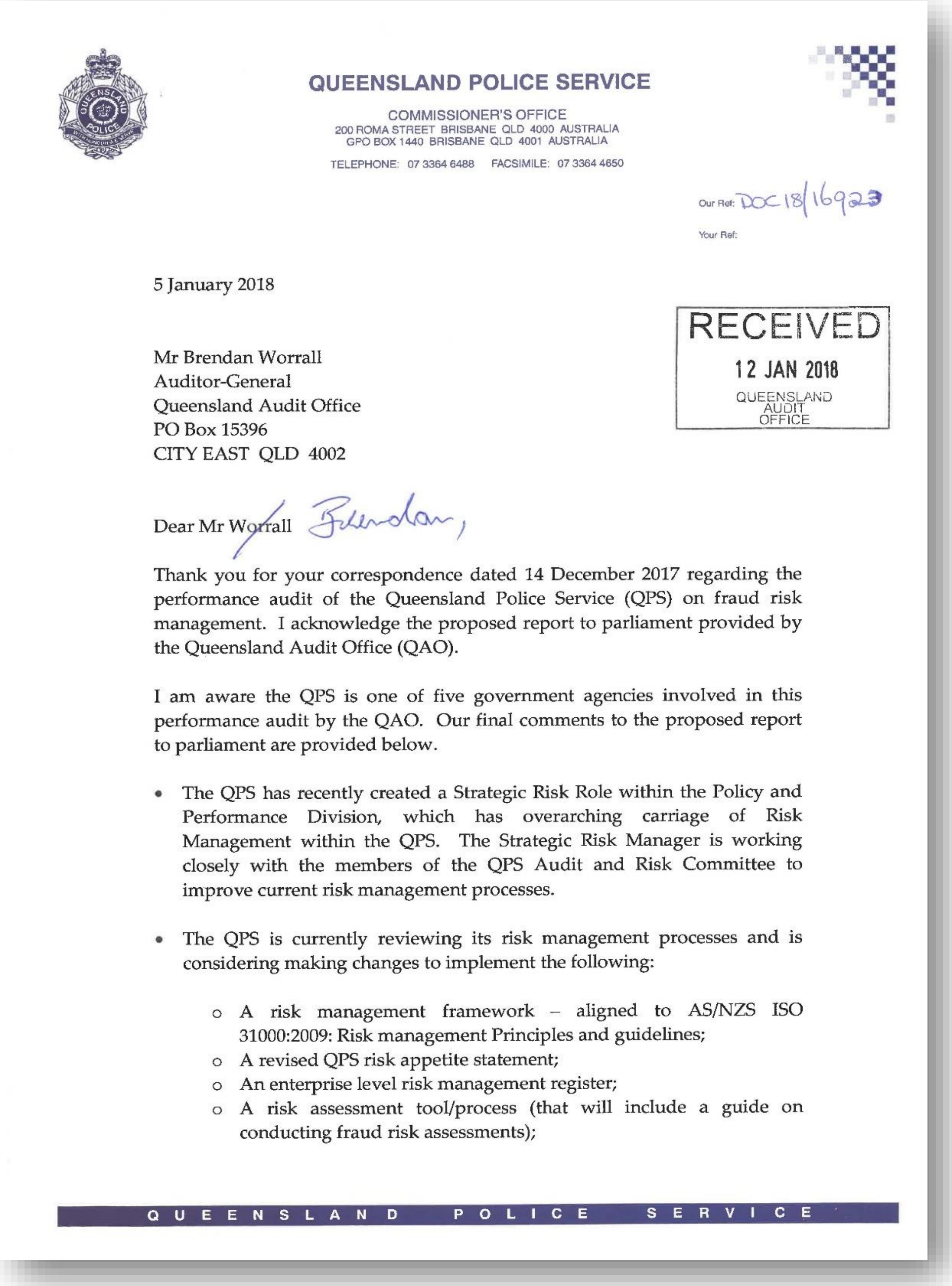
Appendix A—Full responses from agencies

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to the Queensland Police Service, Public Safety Business Agency, Queensland Rail, Queensland Building and Construction Commission and Queensland Fire and Emergency Services.

The heads of these agencies are responsible for the accuracy, fairness and balance of their comments.

This appendix contains their detailed responses to our audit recommendations.

Comments received from Commissioner, Queensland Police Service



QUEENSLAND POLICE SERVICE

COMMISSIONER'S OFFICE
200 ROMA STREET BRISBANE QLD 4000 AUSTRALIA
GPO BOX 1440 BRISBANE QLD 4001 AUSTRALIA

TELEPHONE: 07 3364 6488 FACSIMILE: 07 3364 4650

Our Ref: DOC18/16923
Your Ref:

5 January 2018

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr ~~Worrall~~ Brendan,

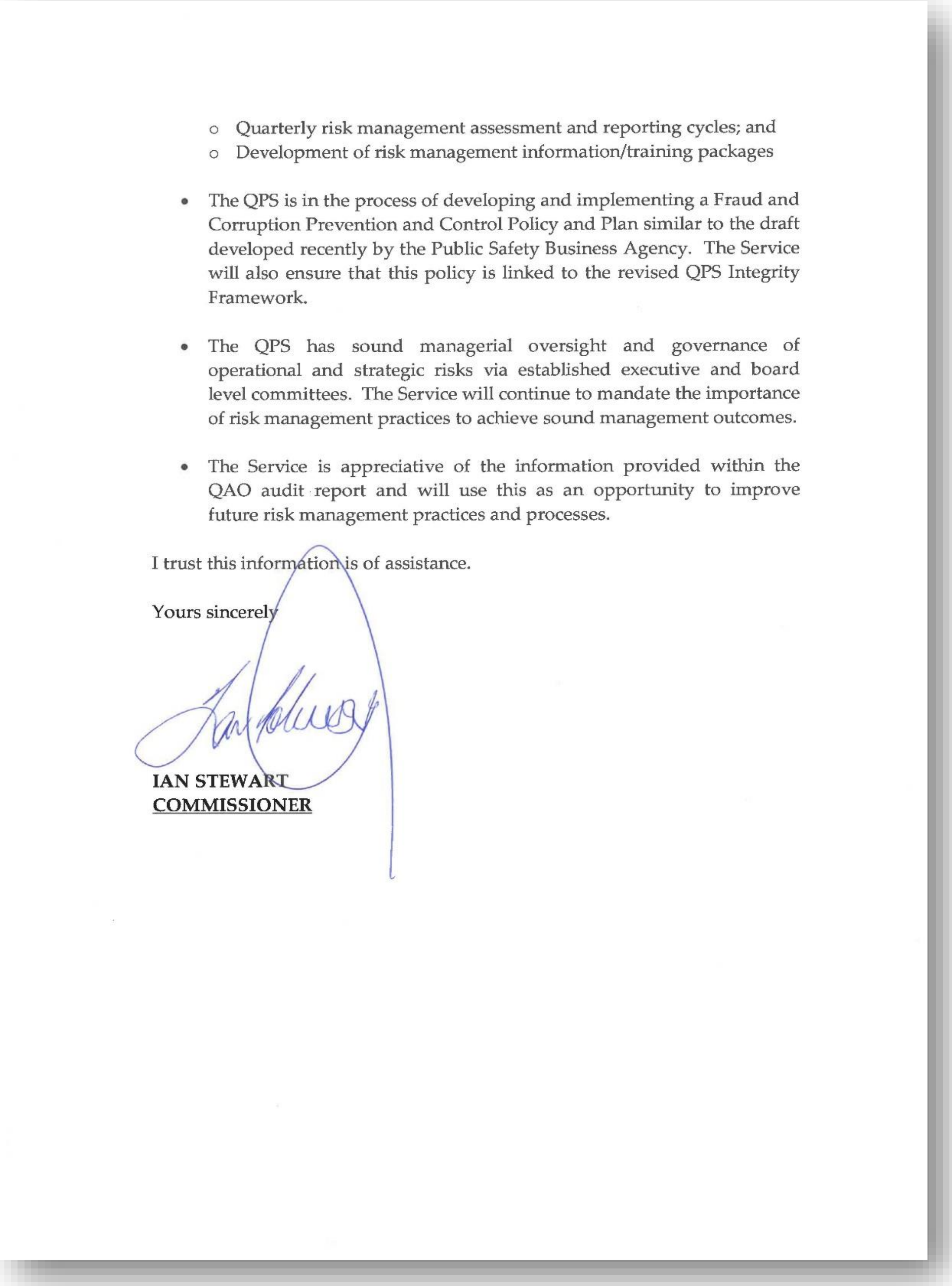
Thank you for your correspondence dated 14 December 2017 regarding the performance audit of the Queensland Police Service (QPS) on fraud risk management. I acknowledge the proposed report to parliament provided by the Queensland Audit Office (QAO).

I am aware the QPS is one of five government agencies involved in this performance audit by the QAO. Our final comments to the proposed report to parliament are provided below.

- The QPS has recently created a Strategic Risk Role within the Policy and Performance Division, which has overarching carriage of Risk Management within the QPS. The Strategic Risk Manager is working closely with the members of the QPS Audit and Risk Committee to improve current risk management processes.

- The QPS is currently reviewing its risk management processes and is considering making changes to implement the following:
  - A risk management framework – aligned to AS/NZS ISO 31000:2009: Risk management Principles and guidelines;
  - A revised QPS risk appetite statement;
  - An enterprise level risk management register;
  - A risk assessment tool/process (that will include a guide on conducting fraud risk assessments);

QUEENSLAND POLICE SERVICE



  - Quarterly risk management assessment and reporting cycles; and
  - Development of risk management information/training packages

- The QPS is in the process of developing and implementing a Fraud and Corruption Prevention and Control Policy and Plan similar to the draft developed recently by the Public Safety Business Agency. The Service will also ensure that this policy is linked to the revised QPS Integrity Framework.

- The QPS has sound managerial oversight and governance of operational and strategic risks via established executive and board level committees. The Service will continue to mandate the importance of risk management practices to achieve sound management outcomes.

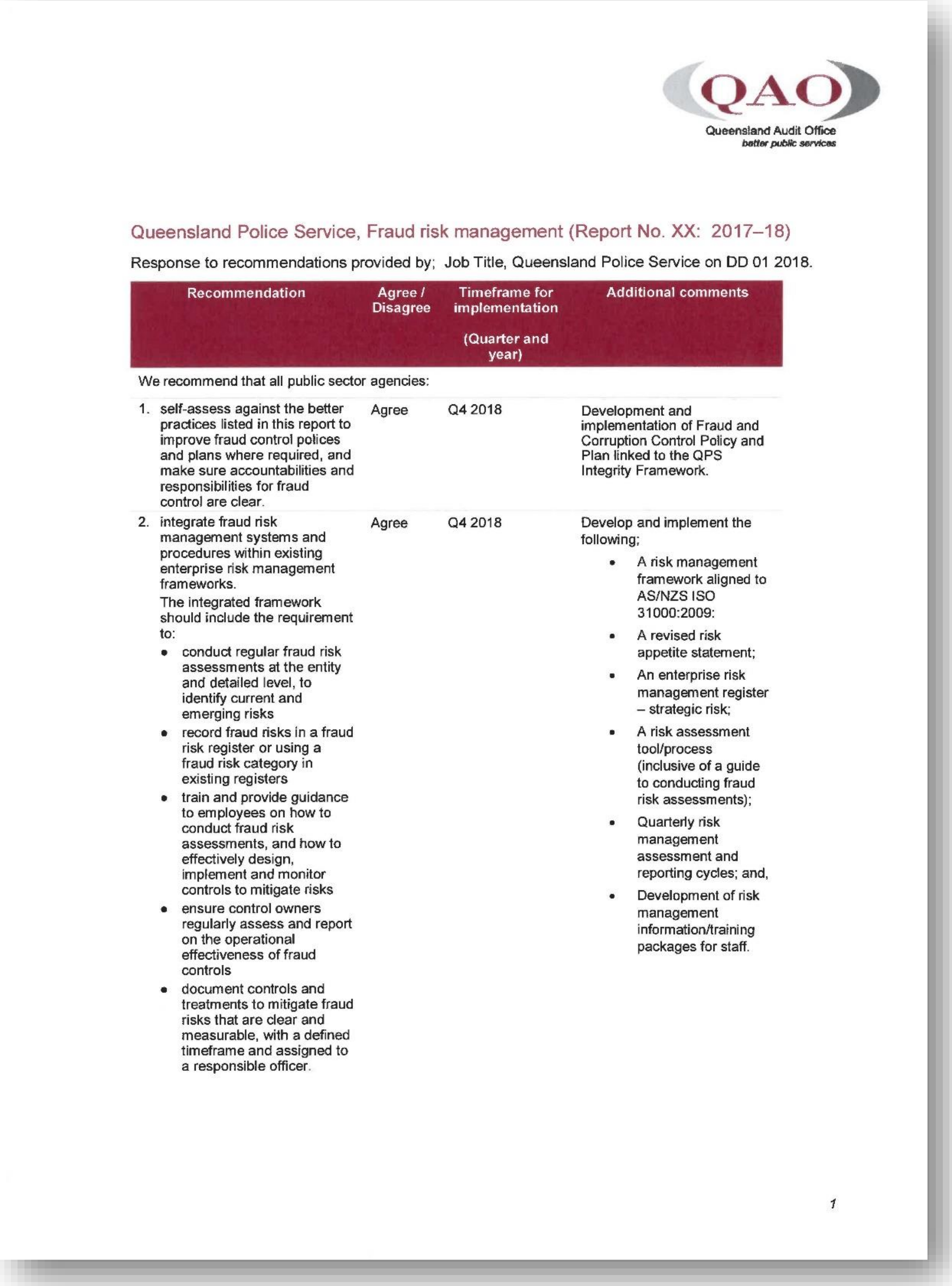
- The Service is appreciative of the information provided within the QAO audit report and will use this as an opportunity to improve future risk management practices and processes.

I trust this information is of assistance.

Yours sincerely

IAN STEWART
COMMISSIONER

Responses to recommendations



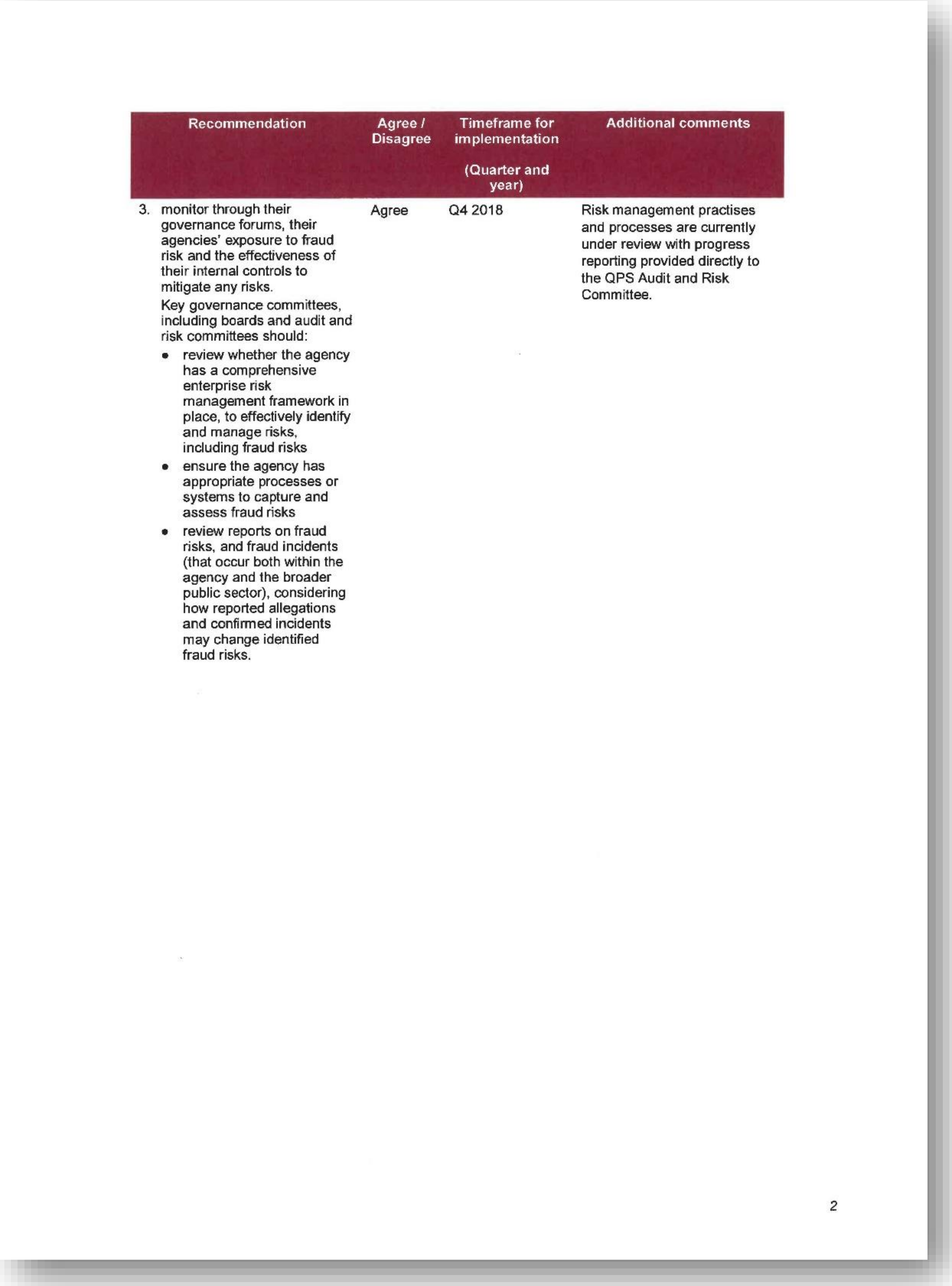
Queensland Audit Office
better public services

Queensland Police Service, Fraud risk management (Report No. XX: 2017–18)

Response to recommendations provided by; Job Title, Queensland Police Service on DD 01 2018.

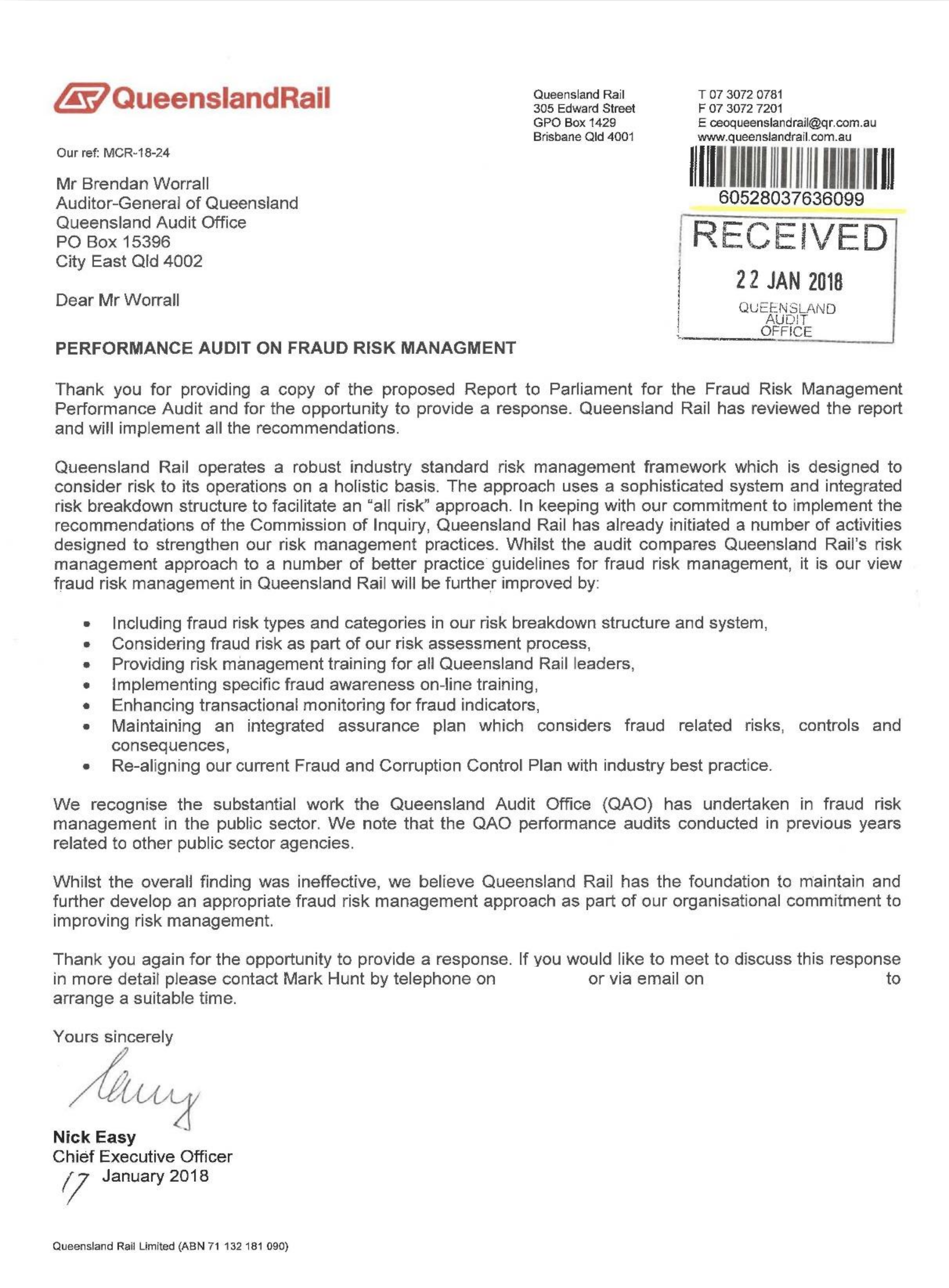
Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that all public sector agencies:			
1. self-assess against the better practices listed in this report to improve fraud control polices and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.	Agree	Q4 2018	Development and implementation of Fraud and Corruption Control Policy and Plan linked to the QPS Integrity Framework.
2. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to: • conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks • record fraud risks in a fraud risk register or using a fraud risk category in existing registers • train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks • ensure control owners regularly assess and report on the operational effectiveness of fraud controls • document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.	Agree	Q4 2018	Develop and implement the following; • A risk management framework aligned to AS/NZS ISO 31000:2009: • A revised risk appetite statement; • An enterprise risk management register – strategic risk; • A risk assessment tool/process (inclusive of a guide to conducting fraud risk assessments); • Quarterly risk management assessment and reporting cycles; and, • Development of risk management information/training packages for staff.

1



Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
3. monitor through their governance forums, their agencies' exposure to fraud risk and the effectiveness of their internal controls to mitigate any risks. Key governance committees, including boards and audit and risk committees should: • review whether the agency has a comprehensive enterprise risk management framework in place, to effectively identify and manage risks, including fraud risks • ensure the agency has appropriate processes or systems to capture and assess fraud risks • review reports on fraud risks, and fraud incidents (that occur both within the agency and the broader public sector), considering how reported allegations and confirmed incidents may change identified fraud risks.	Agree	Q4 2018	Risk management practises and processes are currently under review with progress reporting provided directly to the QPS Audit and Risk Committee.

Comments received from Chief Executive Officer, Queensland Rail Limited



QueenslandRail

Queensland Rail
305 Edward Street
GPO Box 1429
Brisbane Qld 4001

T 07 3072 0781
F 07 3072 7201
E ceoqueenslandrail@qr.com.au
www.queenslandrail.com.au

Our ref: MCR-18-24

Mr Brendan Worrall
Auditor-General of Queensland
Queensland Audit Office
PO Box 15396
City East Qld 4002

Dear Mr Worrall

PERFORMANCE AUDIT ON FRAUD RISK MANAGMENT

Thank you for providing a copy of the proposed Report to Parliament for the Fraud Risk Management Performance Audit and for the opportunity to provide a response. Queensland Rail has reviewed the report and will implement all the recommendations.

Queensland Rail operates a robust industry standard risk management framework which is designed to consider risk to its operations on a holistic basis. The approach uses a sophisticated system and integrated risk breakdown structure to facilitate an “all risk” approach. In keeping with our commitment to implement the recommendations of the Commission of Inquiry, Queensland Rail has already initiated a number of activities designed to strengthen our risk management practices. Whilst the audit compares Queensland Rail’s risk management approach to a number of better practice guidelines for fraud risk management, it is our view fraud risk management in Queensland Rail will be further improved by:

- Including fraud risk types and categories in our risk breakdown structure and system,
- Considering fraud risk as part of our risk assessment process,
- Providing risk management training for all Queensland Rail leaders,
- Implementing specific fraud awareness on-line training,
- Enhancing transactional monitoring for fraud indicators,
- Maintaining an integrated assurance plan which considers fraud related risks, controls and consequences,
- Re-aligning our current Fraud and Corruption Control Plan with industry best practice.

We recognise the substantial work the Queensland Audit Office (QAO) has undertaken in fraud risk management in the public sector. We note that the QAO performance audits conducted in previous years related to other public sector agencies.

Whilst the overall finding was ineffective, we believe Queensland Rail has the foundation to maintain and further develop an appropriate fraud risk management approach as part of our organisational commitment to improving risk management.

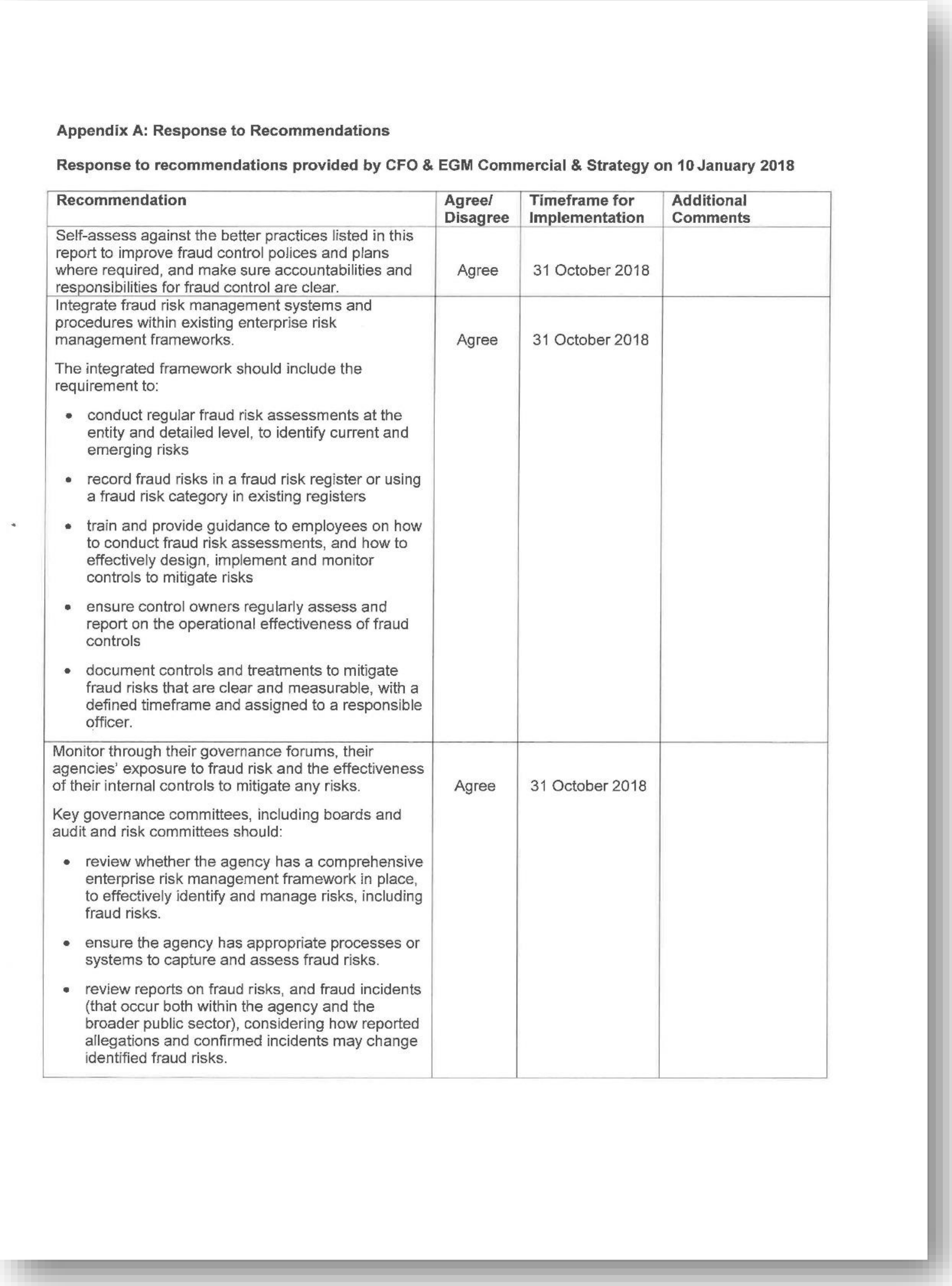
Thank you again for the opportunity to provide a response. If you would like to meet to discuss this response in more detail please contact Mark Hunt by telephone on or via email on to arrange a suitable time.

Yours sincerely

Nick Easy
Chief Executive Officer
17 January 2018

Queensland Rail Limited (ABN 71 132 181 090)

Responses to recommendations

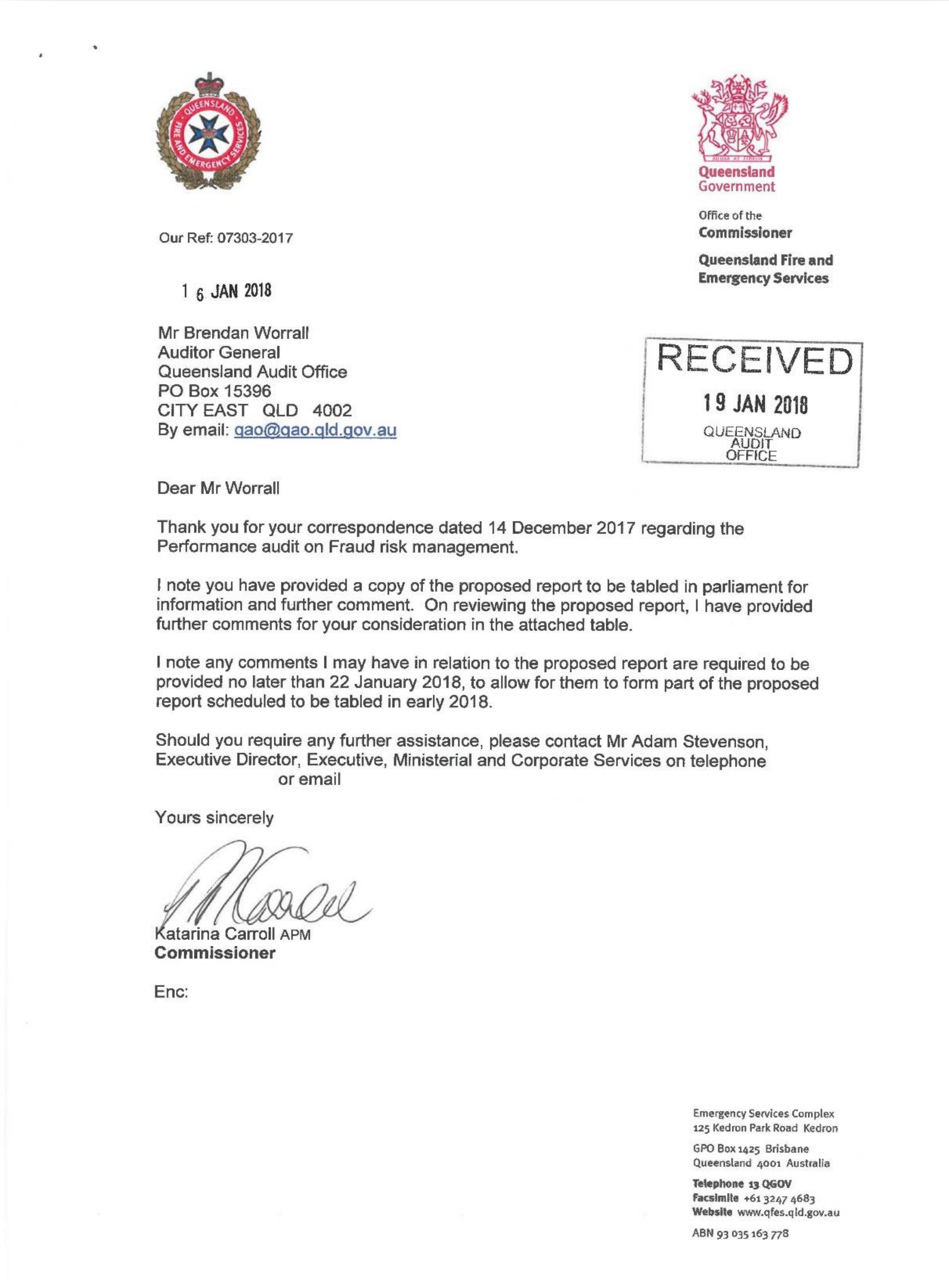


Appendix A: Response to Recommendations

Response to recommendations provided by CFO & EGM Commercial & Strategy on 10 January 2018

Recommendation	Agree/ Disagree	Timeframe for Implementation	Additional Comments
Self-assess against the better practices listed in this report to improve fraud control polices and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.	Agree	31 October 2018	
Integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to: • conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks • record fraud risks in a fraud risk register or using a fraud risk category in existing registers • train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks • ensure control owners regularly assess and report on the operational effectiveness of fraud controls • document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.	Agree	31 October 2018	
Monitor through their governance forums, their agencies' exposure to fraud risk and the effectiveness of their internal controls to mitigate any risks. Key governance committees, including boards and audit and risk committees should: • review whether the agency has a comprehensive enterprise risk management framework in place, to effectively identify and manage risks, including fraud risks. • ensure the agency has appropriate processes or systems to capture and assess fraud risks. • review reports on fraud risks, and fraud incidents (that occur both within the agency and the broader public sector), considering how reported allegations and confirmed incidents may change identified fraud risks.	Agree	31 October 2018	

Comments received from Commissioner, Queensland Fire and Emergency Services



Queensland Government

Office of the
Commissioner

Queensland Fire and Emergency Services

Our Ref: 07303-2017

16 JAN 2018

Mr Brendan Worrall
Auditor General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002
By email: qao@qao.qld.gov.au

Dear Mr Worrall

Thank you for your correspondence dated 14 December 2017 regarding the Performance audit on Fraud risk management.

I note you have provided a copy of the proposed report to be tabled in parliament for information and further comment. On reviewing the proposed report, I have provided further comments for your consideration in the attached table.

I note any comments I may have in relation to the proposed report are required to be provided no later than 22 January 2018, to allow for them to form part of the proposed report scheduled to be tabled in early 2018.

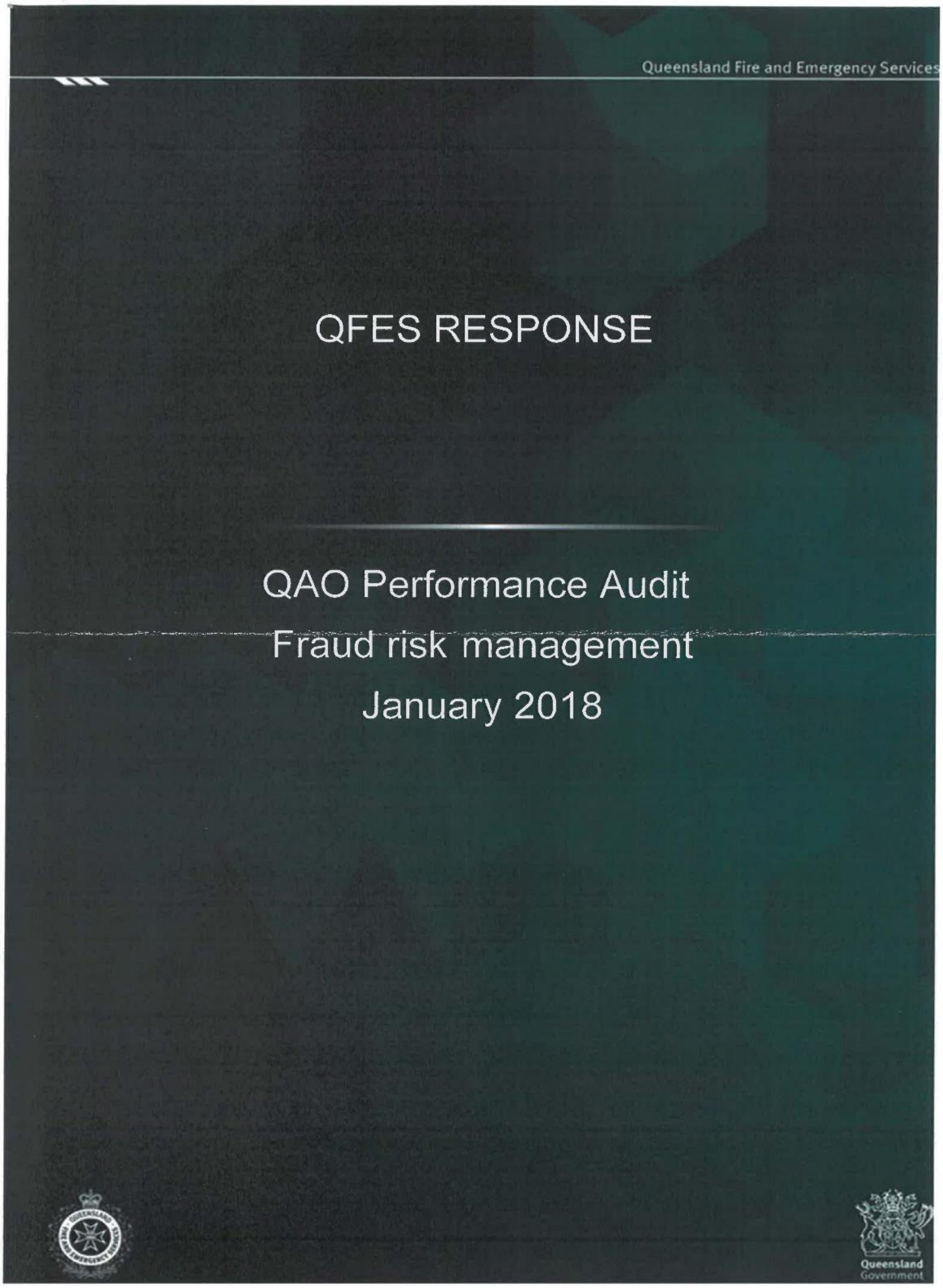
Should you require any further assistance, please contact Mr Adam Stevenson, Executive Director, Executive, Ministerial and Corporate Services on telephone or email

Yours sincerely

Katarina Carroll APM
Commissioner

Enc:

Emergency Services Complex
125 Kedron Park Road Kedron
GPO Box 1425 Brisbane
Queensland 4001 Australia
Telephone 13 QGOV
Facsimile +61 3247 4683
Website www.qfes.qld.gov.au
ABN 93 035 163 778



Queensland Fire and Emergency Services

QFES RESPONSE

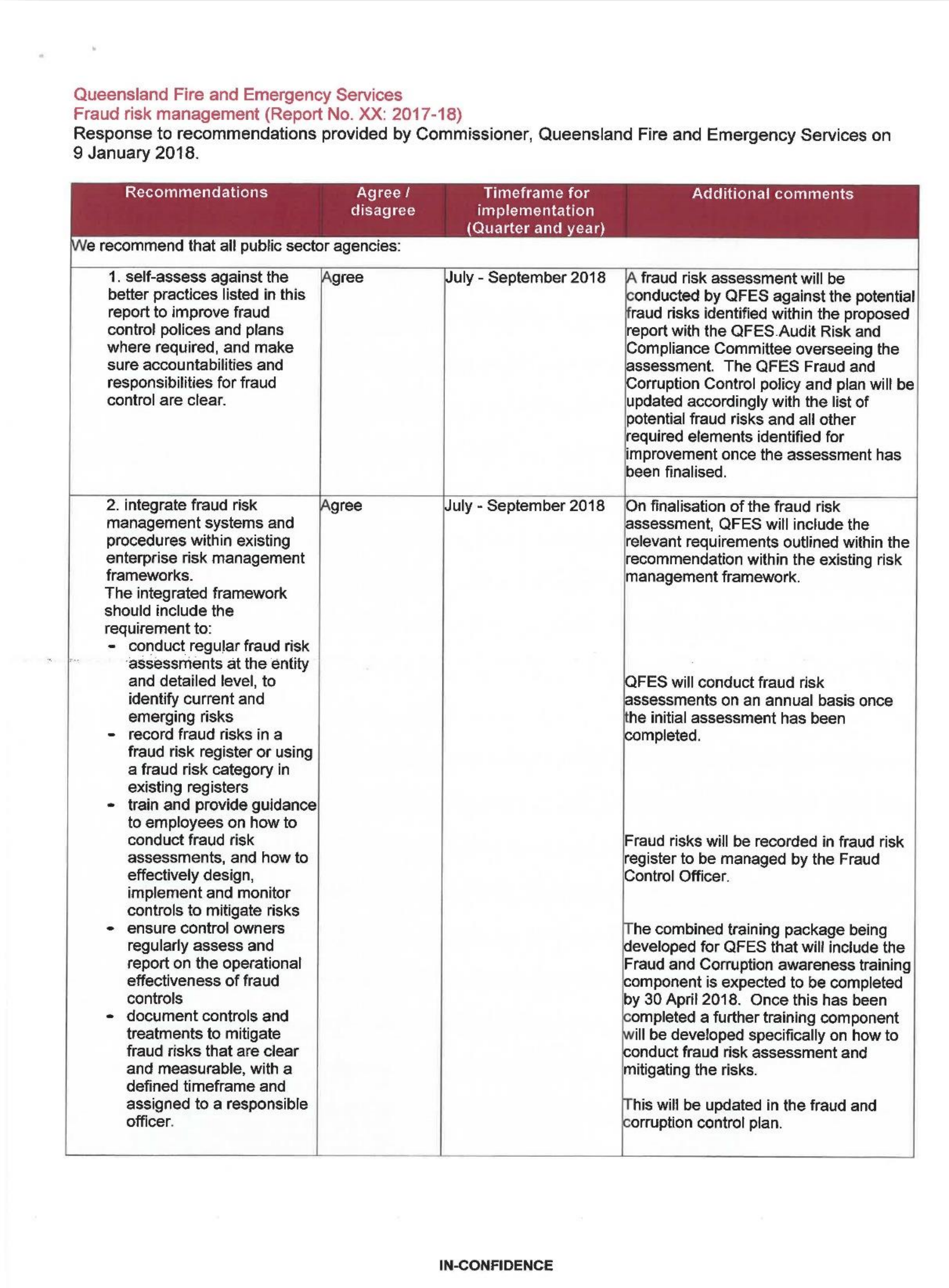
QAO Performance Audit

Fraud risk management

January 2018

Queensland Government

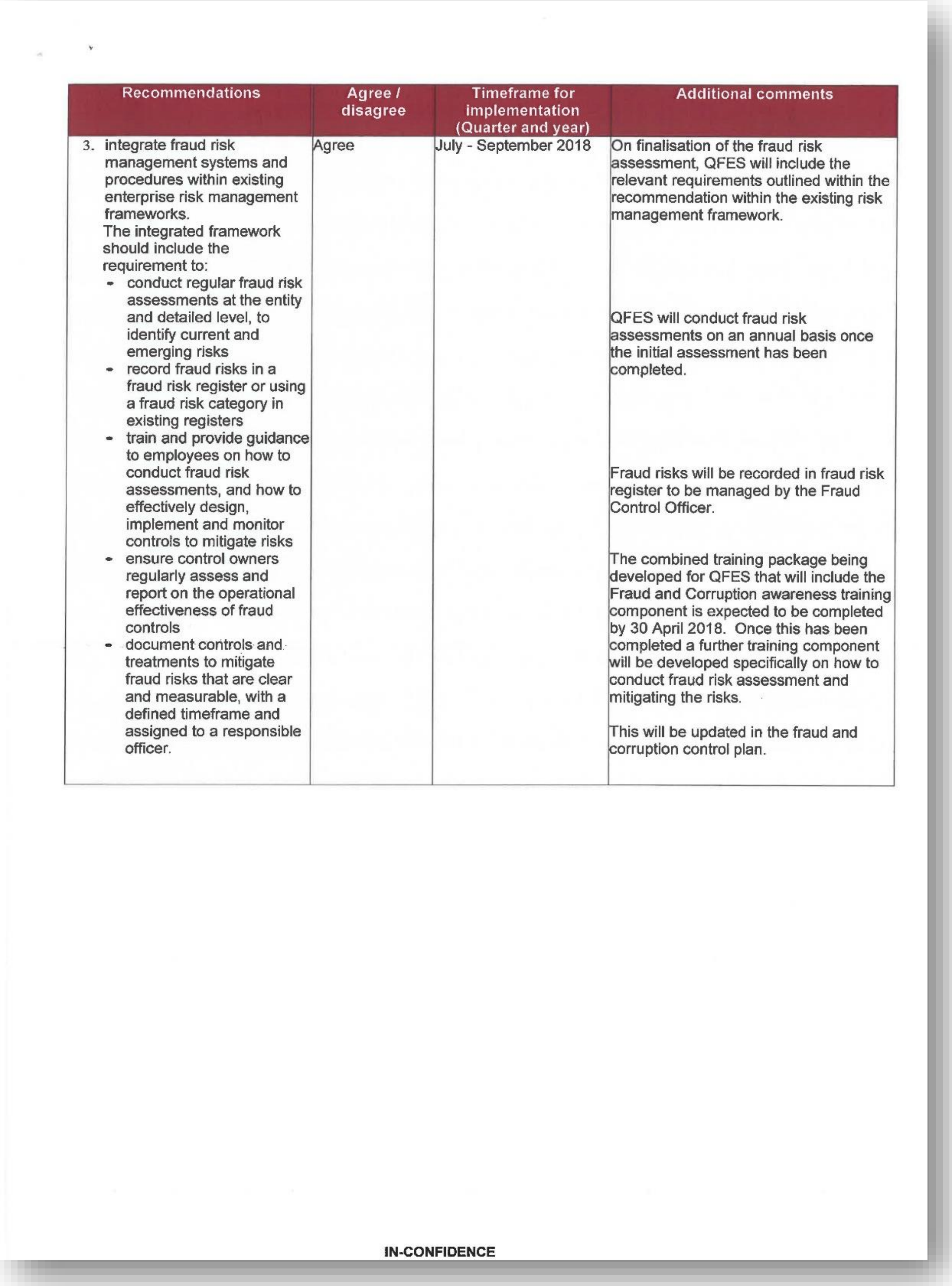
Responses to recommendations



Queensland Fire and Emergency Services
Fraud risk management (Report No. XX: 2017-18)
Response to recommendations provided by Commissioner, Queensland Fire and Emergency Services on 9 January 2018.

Recommendations	Agree / disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that all public sector agencies:			
1. self-assess against the better practices listed in this report to improve fraud control polices and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.	Agree	July - September 2018	A fraud risk assessment will be conducted by QFES against the potential fraud risks identified within the proposed report with the QFES Audit Risk and Compliance Committee overseeing the assessment. The QFES Fraud and Corruption Control policy and plan will be updated accordingly with the list of potential fraud risks and all other required elements identified for improvement once the assessment has been finalised.
2. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to: - conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks - record fraud risks in a fraud risk register or using a fraud risk category in existing registers - train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks - ensure control owners regularly assess and report on the operational effectiveness of fraud controls - document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.	Agree	July - September 2018	On finalisation of the fraud risk assessment, QFES will include the relevant requirements outlined within the recommendation within the existing risk management framework. QFES will conduct fraud risk assessments on an annual basis once the initial assessment has been completed. Fraud risks will be recorded in fraud risk register to be managed by the Fraud Control Officer. The combined training package being developed for QFES that will include the Fraud and Corruption awareness training component is expected to be completed by 30 April 2018. Once this has been completed a further training component will be developed specifically on how to conduct fraud risk assessment and mitigating the risks. This will be updated in the fraud and corruption control plan.

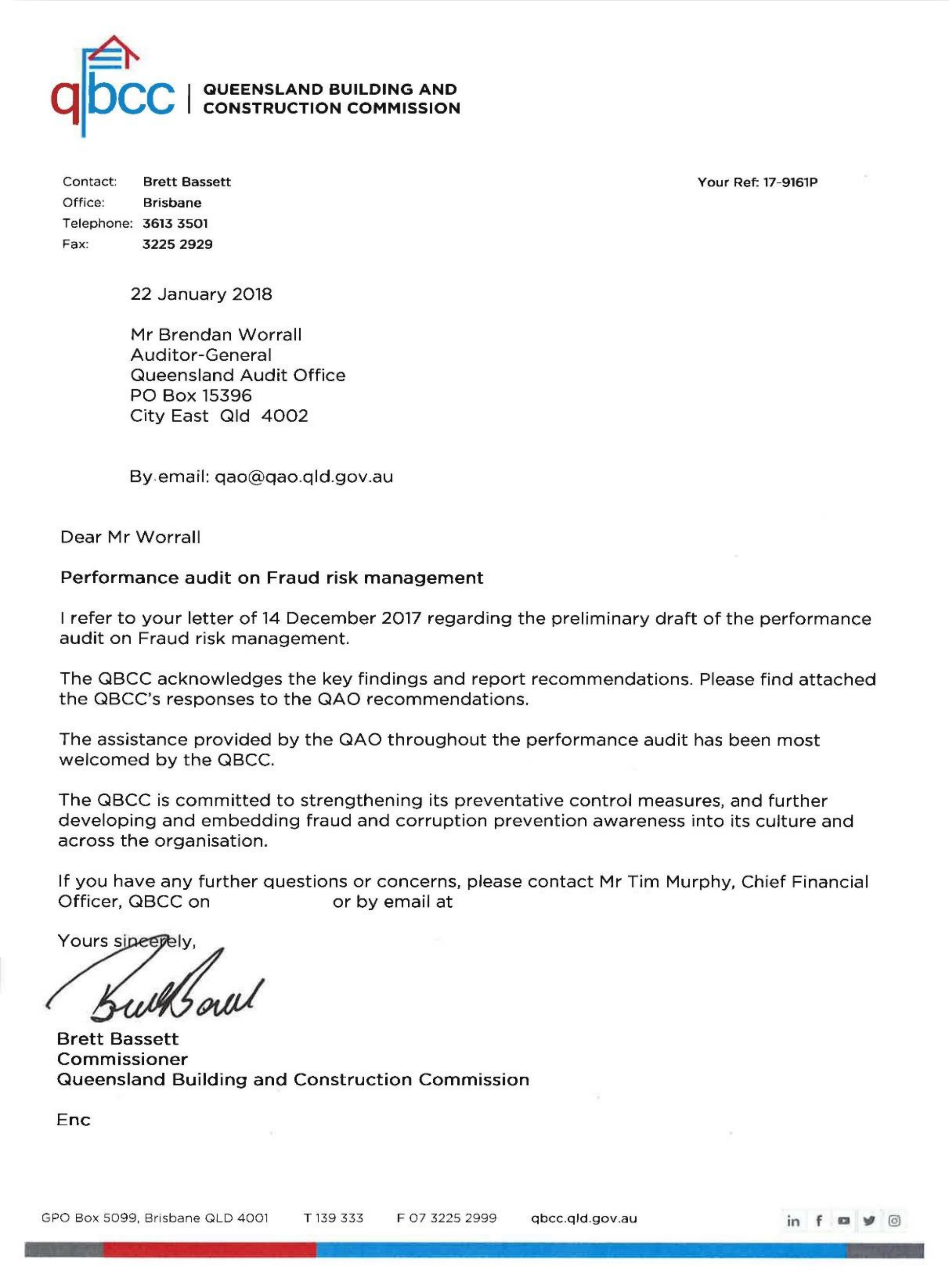
IN-CONFIDENCE



Recommendations	Agree / disagree	Timeframe for implementation (Quarter and year)	Additional comments
3. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to: - conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks - record fraud risks in a fraud risk register or using a fraud risk category in existing registers - train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks - ensure control owners regularly assess and report on the operational effectiveness of fraud controls - document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.	Agree	July - September 2018	On finalisation of the fraud risk assessment, QFES will include the relevant requirements outlined within the recommendation within the existing risk management framework. QFES will conduct fraud risk assessments on an annual basis once the initial assessment has been completed. Fraud risks will be recorded in fraud risk register to be managed by the Fraud Control Officer. The combined training package being developed for QFES that will include the Fraud and Corruption awareness training component is expected to be completed by 30 April 2018. Once this has been completed a further training component will be developed specifically on how to conduct fraud risk assessment and mitigating the risks. This will be updated in the fraud and corruption control plan.

IN-CONFIDENCE

Comments received from Commissioner, Queensland Building and Construction Commission



QUEENSLAND BUILDING AND CONSTRUCTION COMMISSION

Contact: Brett Bassett
Office: Brisbane
Telephone: 3613 3501
Fax: 3225 2929

Your Ref: 17-9161P

22 January 2018

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
PO Box 15396
City East Qld 4002

By email: qao@qao.qld.gov.au

Dear Mr Worrall

Performance audit on Fraud risk management

I refer to your letter of 14 December 2017 regarding the preliminary draft of the performance audit on Fraud risk management.

The QBCC acknowledges the key findings and report recommendations. Please find attached the QBCC's responses to the QAO recommendations.

The assistance provided by the QAO throughout the performance audit has been most welcomed by the QBCC.

The QBCC is committed to strengthening its preventative control measures, and further developing and embedding fraud and corruption prevention awareness into its culture and across the organisation.

If you have any further questions or concerns, please contact Mr Tim Murphy, Chief Financial Officer, QBCC on or by email at

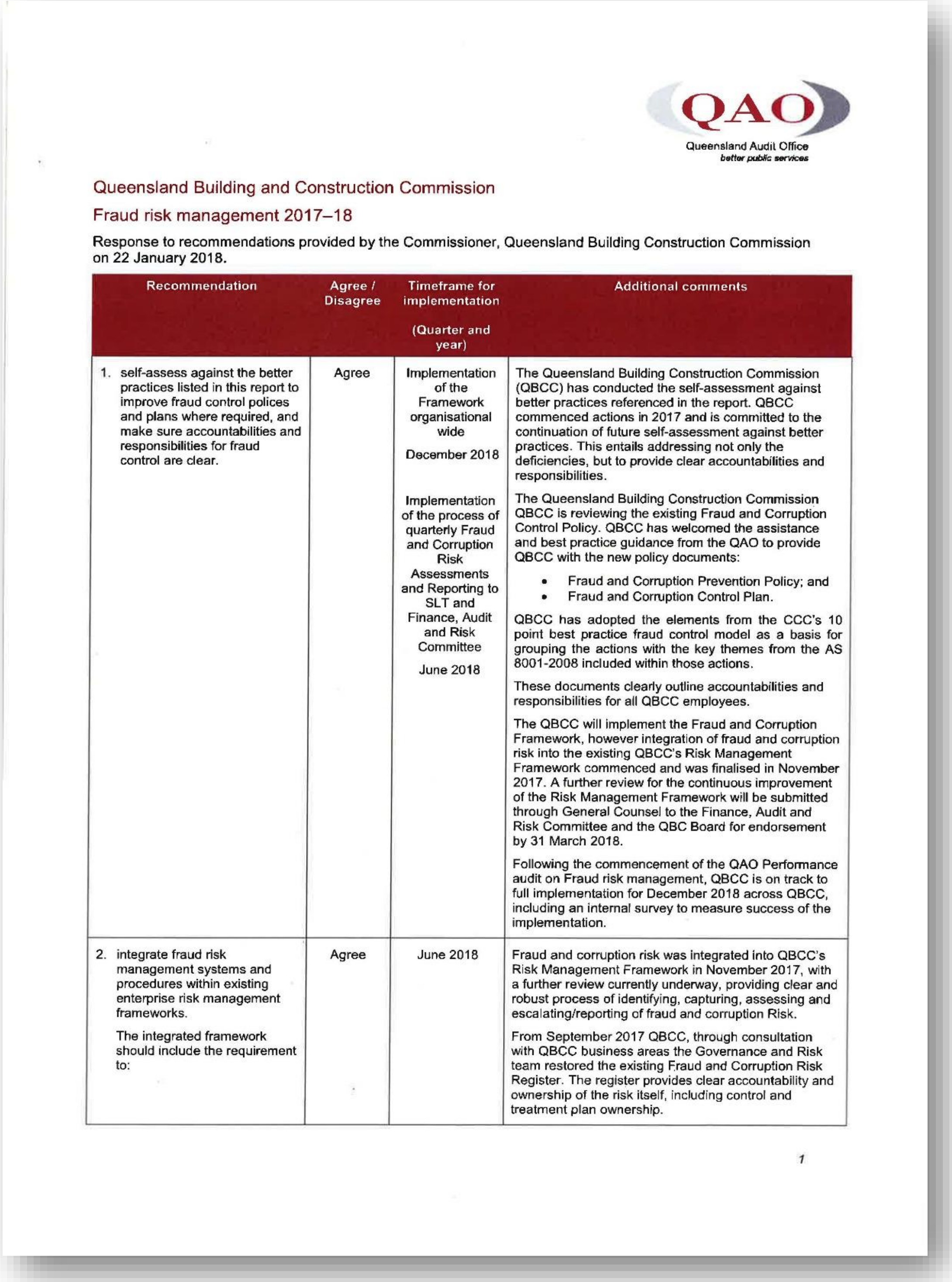
Yours sincerely,

Brett Bassett
Commissioner
Queensland Building and Construction Commission

Enc

GPO Box 5099, Brisbane QLD 4001 T 139 333 F 07 3225 2999 qbcc.qld.gov.au

Responses to recommendations



Queensland Audit Office
better public services

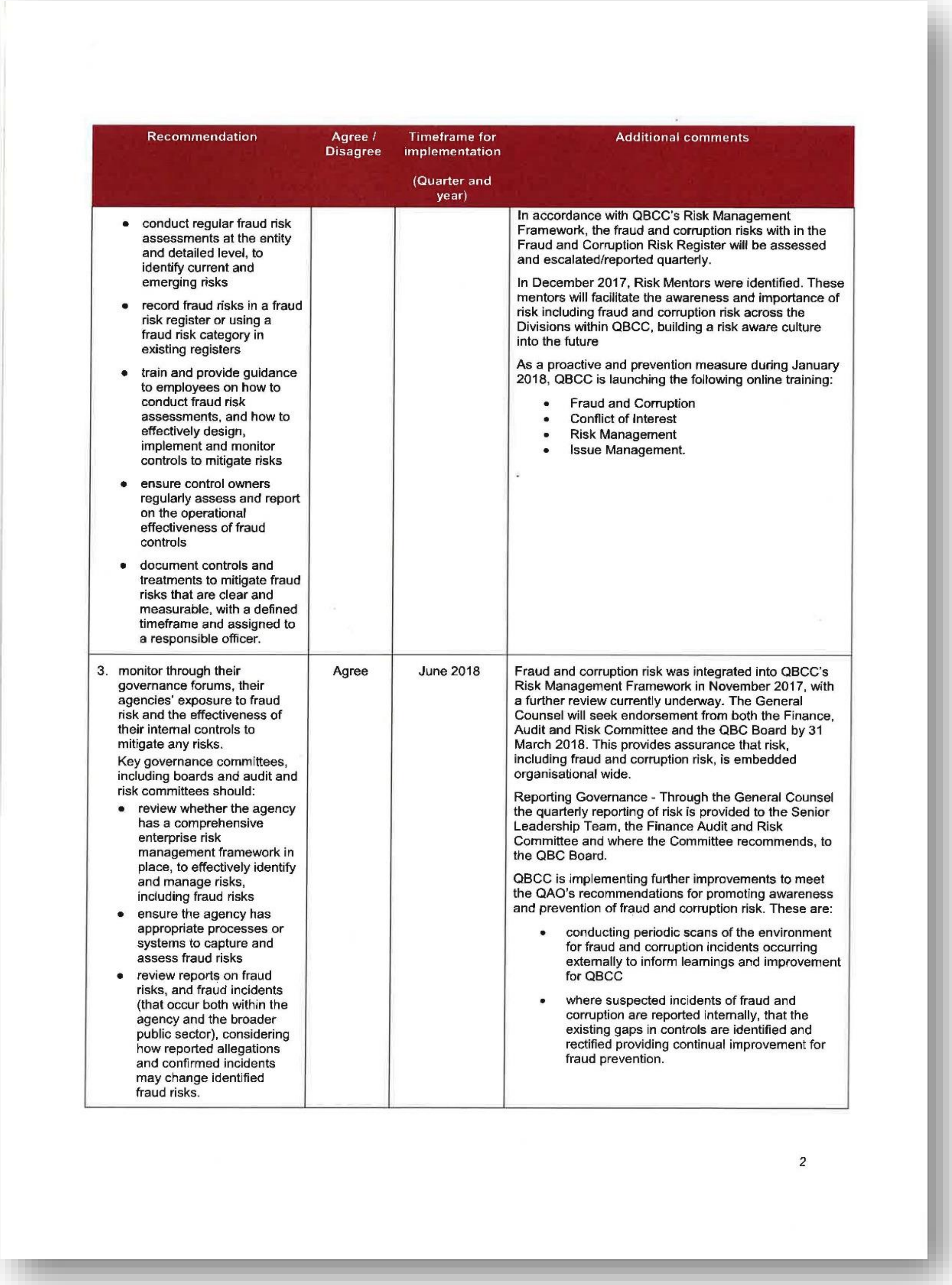
Queensland Building and Construction Commission

Fraud risk management 2017–18

Response to recommendations provided by the Commissioner, Queensland Building Construction Commission on 22 January 2018.

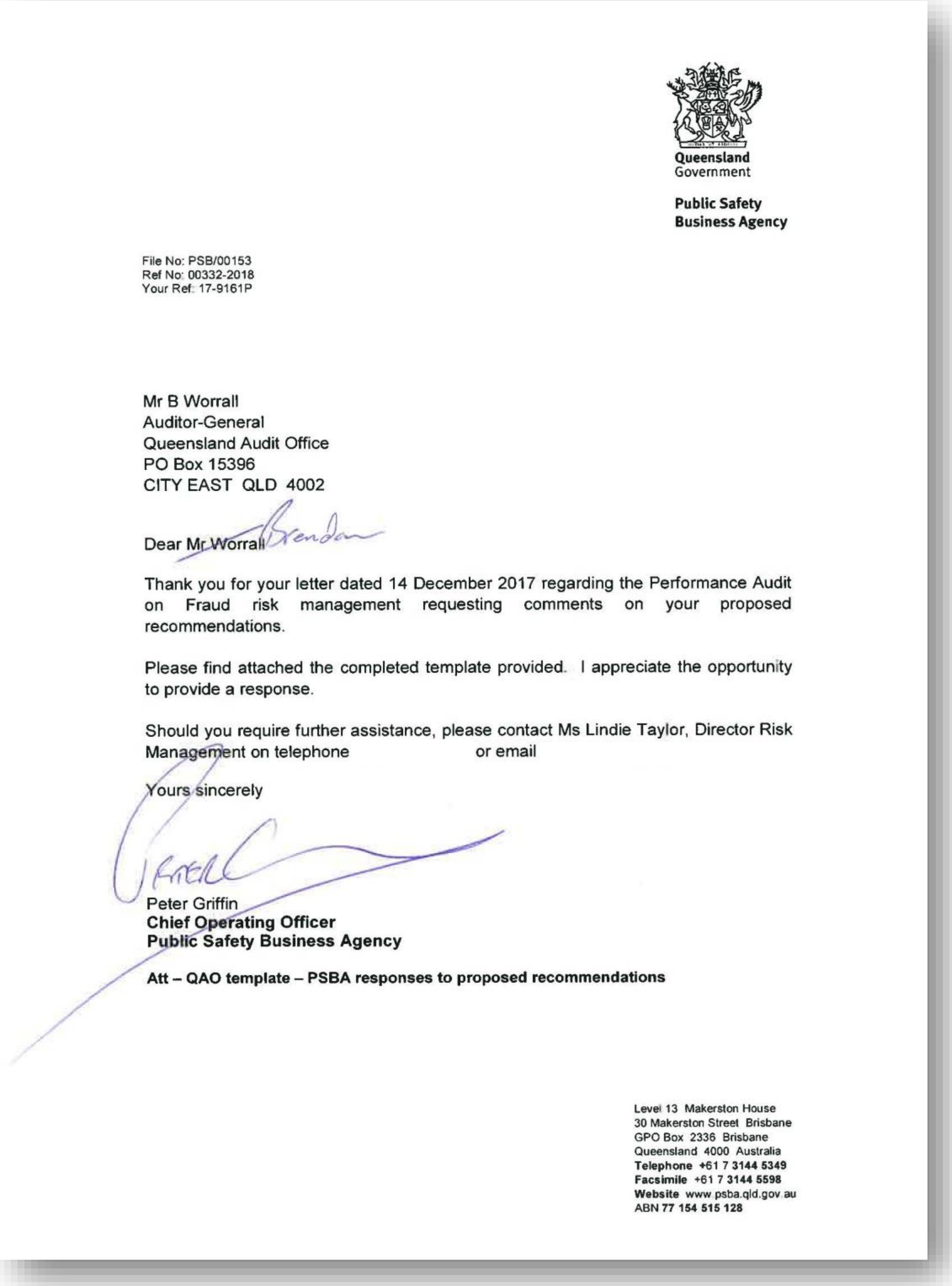
Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
1. self-assess against the better practices listed in this report to improve fraud control polices and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.	Agree	Implementation of the Framework organisational wide December 2018 Implementation of the process of quarterly Fraud and Corruption Risk Assessments and Reporting to SLT and Finance, Audit and Risk Committee June 2018	The Queensland Building Construction Commission (QBCC) has conducted the self-assessment against better practices referenced in the report. QBCC commenced actions in 2017 and is committed to the continuation of future self-assessment against better practices. This entails addressing not only the deficiencies, but to provide clear accountabilities and responsibilities. The Queensland Building Construction Commission QBCC is reviewing the existing Fraud and Corruption Control Policy. QBCC has welcomed the assistance and best practice guidance from the QAO to provide QBCC with the new policy documents: • Fraud and Corruption Prevention Policy; and • Fraud and Corruption Control Plan. QBCC has adopted the elements from the CCC's 10 point best practice fraud control model as a basis for grouping the actions with the key themes from the AS 8001-2008 included within those actions. These documents clearly outline accountabilities and responsibilities for all QBCC employees. The QBCC will implement the Fraud and Corruption Framework, however integration of fraud and corruption risk into the existing QBCC's Risk Management Framework commenced and was finalised in November 2017. A further review for the continuous improvement of the Risk Management Framework will be submitted through General Counsel to the Finance, Audit and Risk Committee and the QBC Board for endorsement by 31 March 2018. Following the commencement of the QAO Performance audit on Fraud risk management, QBCC is on track to full implementation for December 2018 across QBCC, including an internal survey to measure success of the implementation.
2. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to:	Agree	June 2018	Fraud and corruption risk was integrated into QBCC's Risk Management Framework in November 2017, with a further review currently underway, providing clear and robust process of identifying, capturing, assessing and escalating/reporting of fraud and corruption Risk. From September 2017 QBCC, through consultation with QBCC business areas the Governance and Risk team restored the existing Fraud and Corruption Risk Register. The register provides clear accountability and ownership of the risk itself, including control and treatment plan ownership.

1



Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
• conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks • record fraud risks in a fraud risk register or using a fraud risk category in existing registers • train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks • ensure control owners regularly assess and report on the operational effectiveness of fraud controls • document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.			In accordance with QBCC's Risk Management Framework, the fraud and corruption risks with in the Fraud and Corruption Risk Register will be assessed and escalated/reported quarterly. In December 2017, Risk Mentors were identified. These mentors will facilitate the awareness and importance of risk including fraud and corruption risk across the Divisions within QBCC, building a risk aware culture into the future As a proactive and prevention measure during January 2018, QBCC is launching the following online training: • Fraud and Corruption • Conflict of Interest • Risk Management • Issue Management.
3. monitor through their governance forums, their agencies' exposure to fraud risk and the effectiveness of their internal controls to mitigate any risks. Key governance committees, including boards and audit and risk committees should: • review whether the agency has a comprehensive enterprise risk management framework in place, to effectively identify and manage risks, including fraud risks • ensure the agency has appropriate processes or systems to capture and assess fraud risks • review reports on fraud risks, and fraud incidents (that occur both within the agency and the broader public sector), considering how reported allegations and confirmed incidents may change identified fraud risks.	Agree	June 2018	Fraud and corruption risk was integrated into QBCC's Risk Management Framework in November 2017, with a further review currently underway. The General Counsel will seek endorsement from both the Finance, Audit and Risk Committee and the QBC Board by 31 March 2018. This provides assurance that risk, including fraud and corruption risk, is embedded organisational wide. Reporting Governance - Through the General Counsel the quarterly reporting of risk is provided to the Senior Leadership Team, the Finance Audit and Risk Committee and where the Committee recommends, to the QBC Board. QBCC is implementing further improvements to meet the QAO's recommendations for promoting awareness and prevention of fraud and corruption risk. These are: • conducting periodic scans of the environment for fraud and corruption incidents occurring externally to inform learnings and improvement for QBCC • where suspected incidents of fraud and corruption are reported internally, that the existing gaps in controls are identified and rectified providing continual improvement for fraud prevention.

Comments received from Chief Operating Officer, Public Safety Business Agency



Queensland Government

Public Safety Business Agency

File No: PSB/00153
Ref No: 00332-2018
Your Ref: 17-9161P

Mr B Worrall
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear ~~Mr Worrall~~ Brendan

Thank you for your letter dated 14 December 2017 regarding the Performance Audit on Fraud risk management requesting comments on your proposed recommendations.

Please find attached the completed template provided. I appreciate the opportunity to provide a response.

Should you require further assistance, please contact Ms Lindie Taylor, Director Risk Management on telephone or email

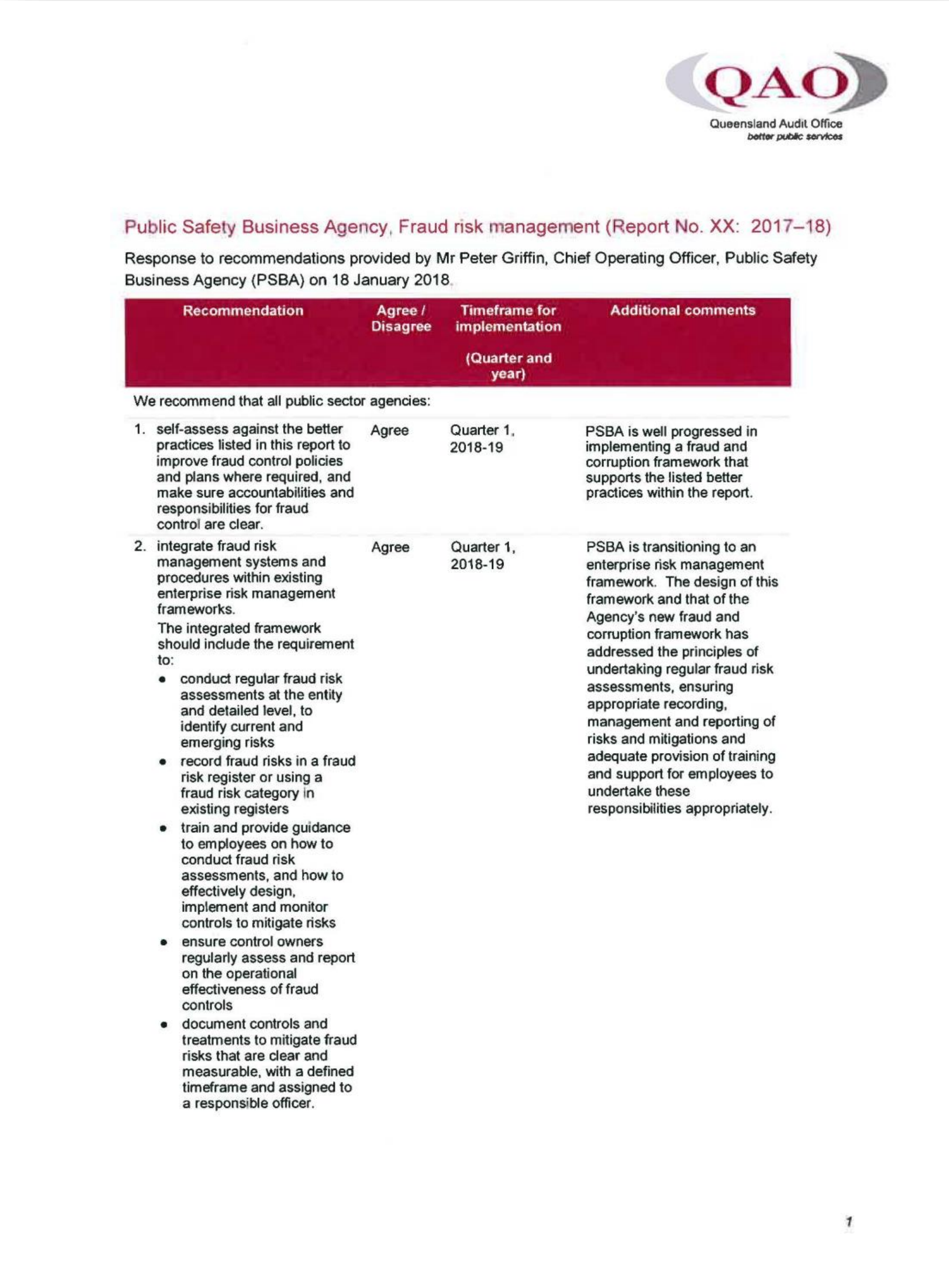
Yours sincerely

Peter Griffin
Chief Operating Officer
Public Safety Business Agency

Att – QAO template – PSBA responses to proposed recommendations

Level 13 Makerston House
30 Makerston Street Brisbane
GPO Box 2336 Brisbane
Queensland 4000 Australia
Telephone +61 7 3144 5349
Facsimile +61 7 3144 5598
Website www.psba.qld.gov.au
ABN 77 154 515 128

Responses to recommendations



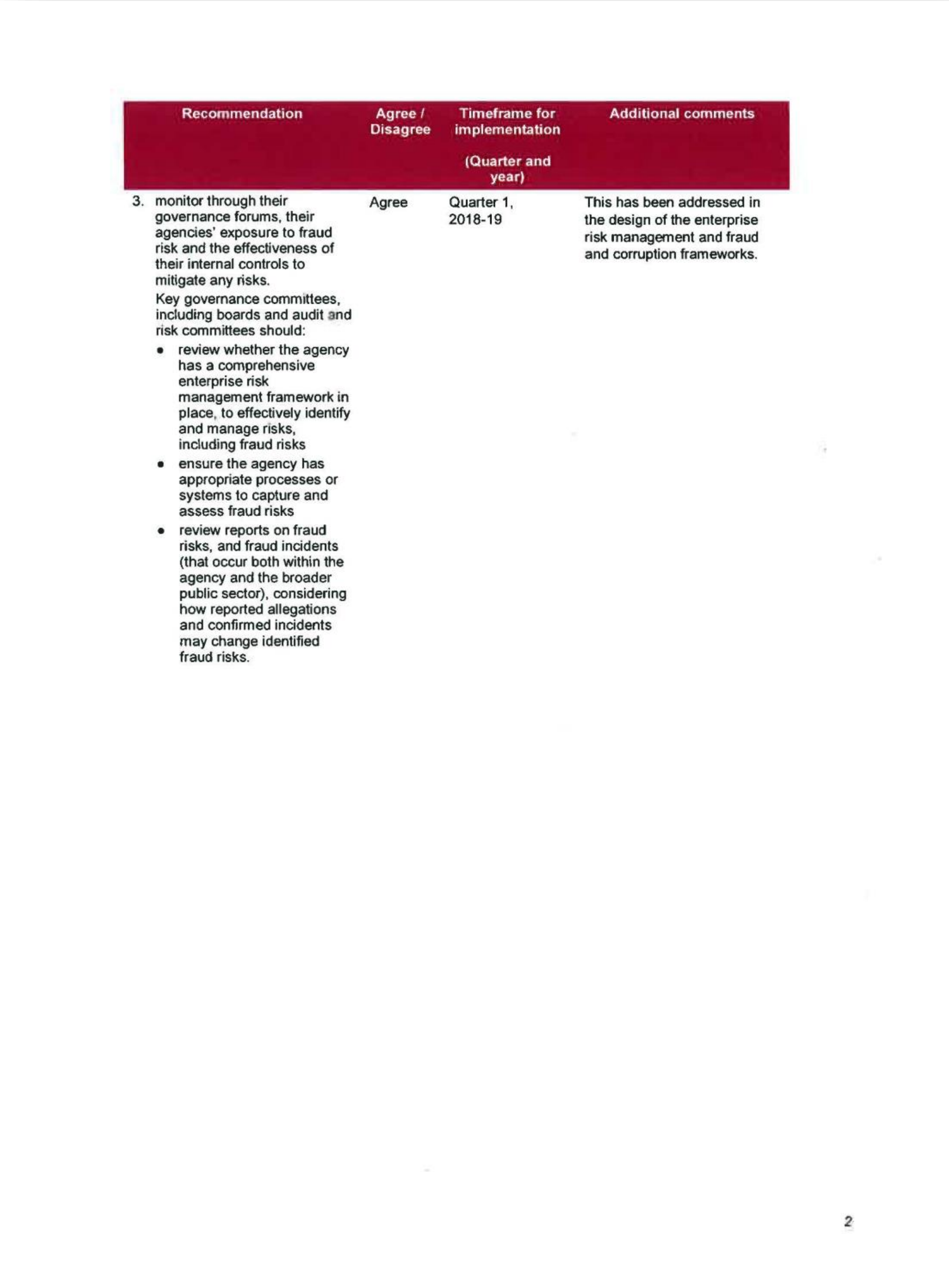
QAO
Queensland Audit Office
better public services

Public Safety Business Agency, Fraud risk management (Report No. XX: 2017–18)

Response to recommendations provided by Mr Peter Griffin, Chief Operating Officer, Public Safety Business Agency (PSBA) on 18 January 2018.

Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that all public sector agencies:			
1. self-assess against the better practices listed in this report to improve fraud control policies and plans where required, and make sure accountabilities and responsibilities for fraud control are clear.	Agree	Quarter 1, 2018-19	PSBA is well progressed in implementing a fraud and corruption framework that supports the listed better practices within the report.
2. integrate fraud risk management systems and procedures within existing enterprise risk management frameworks. The integrated framework should include the requirement to: • conduct regular fraud risk assessments at the entity and detailed level, to identify current and emerging risks • record fraud risks in a fraud risk register or using a fraud risk category in existing registers • train and provide guidance to employees on how to conduct fraud risk assessments, and how to effectively design, implement and monitor controls to mitigate risks • ensure control owners regularly assess and report on the operational effectiveness of fraud controls • document controls and treatments to mitigate fraud risks that are clear and measurable, with a defined timeframe and assigned to a responsible officer.	Agree	Quarter 1, 2018-19	PSBA is transitioning to an enterprise risk management framework. The design of this framework and that of the Agency's new fraud and corruption framework has addressed the principles of undertaking regular fraud risk assessments, ensuring appropriate recording, management and reporting of risks and mitigations and adequate provision of training and support for employees to undertake these responsibilities appropriately.

1



Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
3. monitor through their governance forums, their agencies' exposure to fraud risk and the effectiveness of their internal controls to mitigate any risks. Key governance committees, including boards and audit and risk committees should: • review whether the agency has a comprehensive enterprise risk management framework in place, to effectively identify and manage risks, including fraud risks • ensure the agency has appropriate processes or systems to capture and assess fraud risks • review reports on fraud risks, and fraud incidents (that occur both within the agency and the broader public sector), considering how reported allegations and confirmed incidents may change identified fraud risks.	Agree	Quarter 1, 2018-19	This has been addressed in the design of the enterprise risk management and fraud and corruption frameworks.

Appendix B—Audit objectives and methods

The objective of the audit was to assess whether agencies appropriately identify and assess fraud risks, and apply appropriate risk treatments and control activities to adequately manage their exposure to fraud risks. We assessed if the agencies' plans effectively addressed and targeted fraud risks and if there were any obvious omissions from risk registers.

The audit addressed the objective through the sub-objectives, lines of inquiry and audit criteria outlined in Figure B1.

Figure B1
Audit scope

Sub-objectives	Lines of inquiry	Criteria
1. Do agencies regularly review fraud risks?	1.1. Do agencies perform regular fraud risk assessments?	1.1.1 Agencies have an established framework for fraud and corruption control which outlines the agency's approach to managing risks of fraud and corruption, including policies that set a risk appetite and tolerance levels for the agency.
		1.1.2 Senior management understands its risk exposure, based on its understanding of its inherent risks.
		1.1.3 Agencies perform comprehensive fraud risk assessments regularly in accordance with AS/NZS ISO 31000:2009 to identify, analyse and evaluate fraud risks.
		1.1.4 Agencies record details of fraud risks they identify in their risk register(s) to keep account of all current and emerging fraud risks for the agency.
	1.2. Are assessments sufficient to identify the susceptibility of their business units and services to fraud risk?	1.2.1 Agencies assess fraud risks at the strategic and operational levels to fully understand their fraud risk exposure throughout all areas of the agency.
		1.2.2 Agencies review existing fraud risks regularly to assess if risks are still relevant, or have changed in significance.

Sub-objectives	Lines of inquiry	Criteria
2. Do agencies design and implement appropriate mitigation strategies and risk treatments for identified fraud risks?	2.1. Do appropriate fraud controls exist that will reduce residual fraud risks to an acceptable level?	2.1.1 Agencies' fraud risk controls are designed to match their risk appetite and tolerance levels for the agency.
		2.1.2 Agencies effectively reduce their exposure to fraud risks that are likely to have an impact on service delivery and the achievement of desired outcomes.
	2.2. Are fraud mitigation strategies and risk treatments efficient and effective?	2.2.1 Agency treatment plans and mitigation strategies for each fraud risk effectively reduce risk likelihood and impact within risk tolerances and appetite.
		2.2.2 Agencies use preventative and detective controls appropriately to efficiently mitigate fraud risk to acceptable levels.
3. Do agencies regularly report on and monitor their fraud risk management activities?	3.1. Are fraud risks regularly reported to those charged with governance within the entity and in line with regulatory requirements?	3.1.1 Agencies have appointed a dedicated risk manager (or equivalent) to identify, assess, analyse and monitor agency risks.
		3.1.2 Risk manager (or equivalent) reports on the status of risks (including fraud risks) to inform those charged with governance in a timely manner.
		3.1.3 All frauds perpetuated are reported to the relevant agencies including the Auditor-General, Crime and Corruption Commission, Queensland Police Service.
	3.2. Do agencies regularly assess if their risk treatment plans and fraud management processes are still effective, considering changes in the agency's business environment?	3.2.1 Agencies can link changes to risk treatment plans and fraud management processes to changes in the agency's business environment.
		3.2.2 Fraud risk control reviews are integrated into strategic planning processes.

Source: Queensland Audit Office.

Appendix C—Fraud risk assessment

To undertake an effective fraud risk assessment, agencies need to first develop a detailed understanding of the context and functions of their business, and criteria for rating identified risks.

Agencies' fraud risk assessments need to consider all types of fraud to understand its potential exposure and design appropriate responses. Agencies should rate their inherent fraud risks using their fraud risk criteria.

We developed a fraud risk assessment tool to provide agencies with a methodology to follow when assessing their inherent fraud risks (risks that exist before considering controls or mitigating factors). We used this tool to identify inherent fraud risks for the five agencies we audited.

We identified 27 potential inherent fraud risks that were common to all agencies in scope. Three of the five agencies have taken steps to consider our identified fraud risks. One has already included some of these in its risk registers, while another is planning to conduct a fraud risk assessment to assess their relevance.

To develop our understanding of the context and functions of the in-scope agencies, we applied a fraud risk susceptibility analysis model, which we originally published in the *Fraud Management in Local Government* (Report 19: 2014–15). The model provides a framework for agencies to assess, at an agency level, the factors that may increase their inherent risk of fraud (Appendix D).

To inform our fraud risk susceptibility analysis and fraud risk assessment, we gathered information from a variety of sources, including:

- walkthroughs and inquiry conducted as part of the planning phase of our audit and by the financial audit team
- annual reports
- websites
- organisation structures
- business unit descriptions
- board and governance committee minutes
- risk registers
- fraud risk policies and plans of other public sector entities.

The 27 potential inherent fraud risks we identified were across seven functional areas—human resources, finance, procurement, payroll, reporting, information security/storage and asset management. The range of functions we identified with inherent fraud risks demonstrates how important it is for agencies to perform a holistic fraud risk assessment. Fraud risk can exist in multiple functions across an agency, and agencies need to think beyond the more familiar finance-related fraud risks. Agencies that perform their fraud risk assessments without input from across their business may leave themselves exposed to fraud risks they did not identify.

The potential risks we identified provide examples of risks agencies could consider when they conduct a fraud risk assessment. Noting that this is based on our assessment, we encourage all public sector agencies to undertake their own fraud risk assessment, reflecting on the potential inherent fraud risks we have identified.

When considering each risk, agencies should include additional columns to record the following:

- assessed inherent risk rating (including consequence and likelihood assessments)
- fraud risk controls
- residual risk rating
- fraud risk treatments
- target risk.

Figure C1 shows the columns agencies should include when they conduct a detailed fraud risk assessment for a business area or service line where a preliminary assessment has determined it is high risk.

Figure C1
Fraud risk assessment—detailed

Fraud risk	Risk factor	Risk description	Assessed inherent risk rating			Fraud risk controls	Residual risk rating	Fraud risk treatments	Target risk
			Consequence	Likelihood	Overall				

Source: Queensland Audit Office.

Figure C2 shows examples of inherent fraud risks which are common to public sector agencies.

Figure C2
Inherent fraud risks common to public sector agencies

Fraud risk	Risk factor	Risk description
Fraudulent procurement by employees or contractors	Employees make procurement decisions for high value work on a regular basis.	Risk of employees fraudulently: ▪ manipulating the value of or adding to an existing approved purchase order ▪ splitting purchases to levels below delegation to avoid the procurement team's oversight ▪ seeking inappropriate exemptions to the tendering processes for purchases ▪ fraudulently manipulating or misstating vendor quotes to disguise larger purchases.
Fraudulent procurement practices by suppliers	The same pool of suppliers may bid for multiple high value jobs with the agency over time.	Risk of suppliers fraudulently: ▪ colluding on tender submissions and deliberately favouring a supplier or increasing prices to spread the benefits and increase the available prices ▪ entering a 'cover bid' for a tender from a linked company without declaring the linked ownership of the competing company.
Employees deliberately over-order goods to keep the surplus for personal gain	Employees are able to request the volume of goods in an order.	Risk that an employee deliberately over orders the volume of goods in routine purchases to use the surplus goods for personal gain.
Fraudulent influence by employee on companies included in panel arrangements	Agencies may use multiple panel arrangements to streamline the procurement process for regular purchase types.	Risk of an employee fraudulently influencing decisions to include related vendors on panels.
Fraudulent contract management by employees	Employees manage ongoing contracts with suppliers.	Risk of employees fraudulently managing ongoing contracts with suppliers by: ▪ falsely claiming for service or goods delivered prior to the event ▪ approving fraudulent variances in construction costs ▪ authorising fraudulent invoices ▪ agreeing to pay invoices and amounts earlier than required ▪ waiving supplier liabilities or obligations included in contracts ▪ modifying contract terms (e.g. unauthorised extension of contracts) ▪ providing inaccurate performance feedback.

Fraud risk	Risk factor	Risk description
Fraudulent use of corporate cards	Agencies provide employees with corporate cards for business transactions.	Risk of employees fraudulently using their corporate cards for: ▪ making personal purchases and processing them as business transactions ▪ circumventing the procurement process to favour a supplier.
Fraudulent recording of time worked to increase overtime and other variable payments	Operational employees often receive a high proportion of their pay in overtime and other variable pay types.	Risk of employees submitting or recording fraudulent information in payroll systems which increase their pay by: ▪ overstating hours worked to claim overtime ▪ claiming allowances they are not entitled to.
Fraudulent manipulation of the rostering process	Operational employees often receive a high proportion of their pay in overtime and penalties.	Risk of employees: ▪ taking shifts which attract higher rates, (e.g. allowances or penalty rates) and then taking fraudulent sick leave during ordinary pay shifts. ▪ colluding with colleagues and supervisors to create rosters which maximise the amount of overtime pay.
Fraudulent changes to employee master data	Agencies process their own or submit documentation to a shared service provider to update their employee master data.	Risk of employees submitting fraudulent forms or not submitting forms to artificially increase their pay, including: ▪ creating a fictional employee ▪ increasing their own salary rates or position ▪ colluding to increase the salaries and wages of another employee.
Fraudulent claim for study assistance or leave	Agencies often pay for or reimburse employees' training or study costs where relevant to their role.	Risk that an employee is receiving assistance or leave for study: ▪ they did not undertake ▪ where they misrepresented the nature of the study or training ▪ where they did not pass the subject/course.

Fraud risk	Risk factor	Risk description
Employee misappropriates assets	Employees are often responsible for a number of valuable operational assets or equipment.	Risk that employee steals or lends assets for personal gain, including: ▪ office equipment ▪ plant and machinery ▪ scrap material ▪ inventory.
Employee misappropriates use of motor vehicles	Agencies may own and operate fleets of motor vehicles.	Risk of an employee using operational vehicles for non-business related travel or to enter into private transactions with the public or business owners.
Fraudulent invoicing by employees or external scammers	Agencies make high value and regular payments to vendors.	Risk of an external scammer or employee submitting false documentation to have bank details of vendors changed to receive payment from the agency on fake or legitimate invoices.
Nepotism in recruitment and selection processes	Employees involved in recruitment may be related to, or friends with, one of the applicants for an open position.	Risk of an employee using their position to influence the outcomes of recruitment processers to favour a related party.
Corruption in internal promotion process	Employees involved in internal promotion decisions may have a personal interest in the outcomes.	Risk of an employee involved in internal promotion decisions using their position to promote a less meritorious candidate to: ▪ solicit bribes from employees ▪ promote a candidate where a conflict of interest exists.
Deliberate manipulation of recruitment selection panels	Management choose selection panels to assess candidates in recruitment decisions.	Risk of a selection committee or other authority stacking a selection panel to achieve their desired outcome in recruitment decisions.

Fraud risk	Risk factor	Risk description
Fraudulent operational reporting by management	Management may have a performance element in their pay or other pressure (e.g. political) to achieve certain operational outcomes.	Risk of management fraudulently manipulating or pressuring subordinates to manipulate their reporting on operational performance.
Fraudulent reporting to meet government imposed FTE limits	Agencies may be required to maintain FTE level in accordance with government policies to limit the growth of the public service.	Risk that management fraudulently report the growth of full-time equivalent employees (FTE) during a reporting period.
Manipulation of financial information to present a better financial result	Management may face pressure to report a balanced budget or show progress in reducing expenditure over a reporting period.	Risk of agencies fraudulently manipulating their financial reporting to achieve desired outcomes by, for example: ▪ understating accrued expenses at year end ▪ overstating accrued revenue at year end ▪ manipulating results of valuations.
Claims for reimbursement for non-work-related expenses	Employees can apply for reimbursement for work-related expenses.	Risk of an employee applying for reimbursements of non-work-related expenses.
False WorkCover claims by employees	Employees may suffer physical or mental injury that is directly related to their work.	Risk of employees making fraudulent claims to WorkCover for compensation of lost wages and expenses and fraudulent use of sick leave for reported injuries sustained at work.
Misusing cab charge vouchers for personal use or profit	Agencies may give their employees cab charge vouchers for use in certain circumstances.	Risk of an employee fraudulently using cab charge vouchers for personal trips or on-selling cab charge vouchers.

Fraud risk	Risk factor	Risk description
Fraudulently awarding a grant or making grant payments outside the terms and conditions of grant agreements	Employees may have delegated authority to award grants or process grant payments when they are due, or milestones are achieved.	Risk of an employee approving grant payments where it was not due, or the grantee did not meet a required milestone. Risk of an employee receiving bribes or kickbacks to award a grant to a particular applicant.
Fraudulent misrepresentations by applicants in recruitment and selection processes	Applications for advertised positions may require a minimum qualification or level of experience.	Risk of an employee or applicant for an advertised position presenting false qualifications, experience or references in their job application.
Employees concealing the corrupt conduct of another employee	Employees or management may observe or be informed of corrupt conduct by another employee.	Risk of an employee or management ignoring or concealing the corrupt or fraudulent conduct of another employee to protect the employee or agency from the repercussions.
Fraudulent disclosure of confidential information by a current or terminated employee	Terminated or current employees may have access to confidential or politically sensitive information in an agencies system or electronically stored (e.g. USB stick).	Risk of a terminated or current employee providing confidential or sensitive information to an interested third party for personal gain.
Fraudulent disposal of information to enable a cover up	Employees that have engaged in or are aware of fraud may have privileged access to delete or destroy documentation and evidence.	Risk of an employee destroying hard or soft copy documentation to cover up fraud or corruption at an agency.

Source: Queensland Audit Office.

Appendix D—Fraud risk susceptibility analysis

Category	Attribute	Factors that increase fraud risk	Fraud exposure
Financial	Materiality of economic flows	High value/low volume, and/or high volume/low value transactions with third parties.	Fraud risk increases in both likelihood and consequence as the sums involved increase.
	Nature of transactions	Non-exchange/non-reciprocal where values given do not match values received, e.g. grants, subsidies, donations, rates and other involuntary transfers.	Unlike a commercial exchange, the inability to readily compare or reconcile the value of what was provided with the value of what was received increases the opportunity for fraud and the likelihood that it remains undetected.
	Susceptibility to manipulation	Accounting balances require subjective measurements involving high levels of judgement or expertise to calculate.	The manipulation of accounting balances can be used to conceal frauds, or may itself be fraudulent by concealing losses or adverse financial positions.
Relationships	Economic dependency	High supplier dependency—supplier relies on the entity for a significant proportion of its gross turnover/continued solvency. High remuneration dependency—salary at risk or other performance incentive schemes with large bonuses or earn-outs arrangements relative to base salary contingent upon achieving targets.	Supplier dependency creates an incentive for the supplier to offer bribes and an opportunity for the purchaser to request kick-backs to retain business. Overly aggressive or unrealistic performance targets can motivate employees to commit fraud to conceal or overstate actual performance, or can be used to rationalise fraud when bonuses are not paid.
	Market depth	Limited market depth restricting competition, existence of oligopoly or monopoly suppliers.	Lack of competition creates opportunities for collusive tendering, and for predatory pricing or other cartel behaviours.
	Proximity to external parties	High degree of direct, face-to-face contact required. Interaction with customers and suppliers at their premises or in the field.	Ongoing personal contact away from direct supervision establishes the opportunity to cultivate inappropriate personal relationships or to groom others to unknowingly facilitate frauds.

Category	Attribute	Factors that increase fraud risk	Fraud exposure
	Related parties	Related party transactions—employees or their spouse, children, and other close relatives or associates have a direct or indirect personal pecuniary interest in transactions or confidential information. Non-commercial, non-arm's length transactions.	Personal interests inherently conflict with public interest and motivate fraudulent behaviour. Transaction values that are not set by reference to observable market inputs create the opportunity for fraud.
Attitudes	Internal controls	Failure to quickly address or remediate internal control issues identified by auditors and other parties. Corner-cutting, failure to follow due process is tolerated or encouraged. Senior leadership does not promote good governance.	Failure by management to demonstrate a commitment to strong and effective control fosters weak control consciousness and a poor control culture that increases the opportunity both for fraud to occur and for it to remain undetected.
	Transparency/accountability	Reluctance to voluntarily disclose information publicly. Limited or poor quality internal reporting to executive.	Failure to acknowledge mistakes, to accept blame and to report risks fosters a culture of secrecy which increases the risk that unusual or suspect transactions and behaviours will not be reported.
Use of assets	Intrinsic value of physical assets	Use of highly ‘portable and attractive’ items of equipment. Handling of cash or other assets readily convertible into cash.	Movable equipment and machinery and items of cash or negotiable instruments are inherently more susceptible to theft or misappropriation by employees.
	Intrinsic value of intangibles	Access to commercially sensitive/economically valuable information not publicly available, e.g. intellectual property.	The intangible nature of sensitive information makes it difficult to secure and to prevent being misused for personal gain or advantage.

Category	Attribute	Factors that increase fraud risk	Fraud exposure
Decision making	Assignment of authority	Decision making is widely devolved to business units. Authority is highly delegated below senior management.	The further removed the approval and scrutiny of transactions are from the 'centre' and from the 'top' of the organisation the greater potential for fraud to remain undetected.
	Decentralisation of operations	Operations in locations remote from central office. Span of management.	The 'tyranny of distance' makes it harder to establish consistent processes and to understand how controls are being applied.
	Discretion	Personal discretion applied in determining allocations to third parties.	Staff or elected officials with the discretion to determine how funds are allocated to third parties have the ability to over-ride standard processes and expose their organisation to fraud.
	Supervision	Span of control is high. No supervisory review before decisions. No centralised monitoring after decisions.	Lack of supervision creates the opportunity for staff to commit fraud and that remains undetected e.g. paying for goods and services that were never received.

Source: Queensland Audit Office.

Auditor-General reports to parliament

Reports tabled in 2017–18

Number	Title	Date tabled in Legislative Assembly
1.	Follow-up of Report 15: 2013–14 Environmental regulation of the resources and waste industries	September 2017
2.	Managing the mental health of Queensland Police employees	October 2017
3.	Rail and ports: 2016–17 results of financial audits	December 2017
4.	Integrated transport planning	December 2017
5.	Water: 2016–17 results of financial audits	December 2017
6.	Fraud risk management	February 2018

Contact the Queensland Audit Office

qao.qld.gov.au/reports-resources/parliament

Suggest a performance audit topic

Contribute to a performance audit in progress

Subscribe to *Insights* now

Connect with QAO on LinkedIn