Crime and Corruption Commission
QUEENSLAND

Corruption audit report

September 2017

Effectiveness of Queensland public sector corruption risk assessments

Summary audit report

Acknowledgments

The CCC acknowledges the cooperation and assistance of participating departments and statutory bodies during this audit.

Crime and Corruption Commission

GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace
Fortitude Valley QLD 4006

Phone: 07 3360 6060
(toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

Note: This publication is accessible through the CCC website <www.ccc.qld.gov.au>.

Contents

Summary

In 2016–17, the CCC received 3049 complaints involving allegations of corruption (one complaint may consist of a number of allegations), up from 2674 complaints in 2015–16. This is an increase of 14 per cent from the preceding financial year.

Queensland public sector agencies have a policy of "zero tolerance" regarding fraudulent or corrupt conduct in their workplace, and are committed to the prevention and management of potential corruption risks. The *Crime and Corruption Act 2001* (CC Act) outlines legislative obligations in relation to corruption. In doing so the CC Act does not place sole responsibility for dealing with corruption on the CCC. Rather it recognises that reducing corruption must form a part of the core business of all public sector agencies.

Prevention initiatives are not optional. Effective risk management and internal controls are required by the *Financial Accountability Act 2009* and the *Financial and Performance Management Standard 2009*. Prevention is also important to upholding the ethics principles and values set out in the *Public Sector Ethics Act 1994*.

To meet its obligations, an agency's approach to managing the risks of fraud and corruption should be underpinned by adequate policy and risk assessment processes directed towards producing effective anti-corruption programs to address particular risks.

In 2016–17 the Crime and Corruption Commission (CCC) conducted an audit of corruption risk assessment processes across six departments and statutory bodies.

The audit identified that these agencies conduct corruption risk assessments that are linked to their risk management framework. All agencies have in place the mechanisms to identify, analyse and evaluate potential corruption risks. The review also identified 12 areas for improvement in agencies' risk assessment processes.

The fraud and corruption control plan that documents each agency's approach to controlling corruption threats and risks at the agency, significant location and business process levels, should include definitions for fraud and corruption, be communicated to all staff, and be reviewed at least once every two years. The audit identified two agencies which fell short in this respect.

The audit also identified that one agency has not assessed its ethical culture, which is a key strategy in managing the risk of fraud and corruption. The reason for conducting an assessment such as this is to provide the agency with information about the overall attitude of its senior executives and employees toward ethical behaviour. This will identify specific locations within the agency's operations which run a higher risk of staff engaging in fraud and corruption.

The CCC's audit identified that two of the agencies reviewed need to prepare risk appetite statements for risk categories, to assist with decisions on how each risk is to be treated. Not all risk types are tolerable.

In the audit, the CCC found that the identification of potential corruption risks, including the significant business areas vulnerable to fraud and corruption, could be improved across the agencies by enhancing assessment processes. Corruption risks can be more difficult to locate and deal with than the risks associated with common fraud incidents. They also affect key operational areas. Corruption manifests in decision-making significantly more than any other activity. To help staff in managing the risks, these potential risks should be communicated widely to promote awareness of vulnerabilities.

Overall, the agencies have sound corruption risk assessment processes in place that enable them to control corruption risks accurately, with enhanced practices proposed for implementation.

Introduction

The CCC has a lead role in helping public sector agencies to deal effectively and appropriately with corruption. Each financial year the CCC conducts a program of audits to determine how agencies have responded to particular types of complaints and how robust their complaints management and corruption prevention frameworks are. The CCC also undertakes audits aimed at controlling the risks of corruption within the public sector.

In 2016–17, the CCC conducted an audit examining how a representative sample of departments and statutory bodies conducted corruption risk assessments.

What is corruption?

Corruption is defined in the CC Act as corrupt conduct or police misconduct. As this audit dealt only with corruption risk assessments involving departments and statutory bodies, further consideration of police misconduct is not required. Corrupt conduct is defined in section 15 of the CC Act and includes conduct by any person which meets all four elements of the section, as described below.

a) **Effect of the conduct:** adversely affects, or could adversely affect, directly or indirectly, the performance of functions or the exercise of powers of an agency; or an individual person holding an appointment in the agency; and

b) **Result of the conduct:** results, or could result, directly or indirectly, in the performance of functions or the exercise of powers mentioned above in a way that—
   - is not honest or is not impartial; or
   - involves a breach of the trust placed in a person holding an appointment, either knowingly or recklessly; or
   - involves a misuse of information or material acquired in or in connection with the performance of functions or the exercise of powers of a person holding an appointment; and

c) **Benefit or detriment arising from the conduct:** is engaged in for the purpose of providing a benefit to the person or another person or causing a detriment to another person; and

d) **Criminal offence or disciplinary breach:** would, if proved, be a criminal offence; or a dismissible disciplinary breach.

Examples of corrupt conduct

- Manipulation of a selection panel by a panel member to ensure that their spouse gets a position even though they are not the most meritorious applicant i.e. nepotism.
- Accessing and/or disclosing official, confidential or personal information for own benefit or the benefit of others i.e. unauthorised access and/or release of information.
- Fraudulently dispersing grant funds to related parties in order to obtain personal gains i.e. fraud.
- Preferential treatment of certain suppliers of services or goods to the agency in return for a monetary consideration or other benefit from the supplier to the agency employee i.e. obtaining a secret commission.

What is corruption risk assessment?

Corruption risk assessment is the systematic identification, analysis and evaluation of corruption risk.

The CCC promotes a three-step process for implementing mechanisms that will assist an agency in effective corruption risk assessments. (Note that the following is not exhaustive and should be considered a summary guide only.)

The three steps consist of:

1 Policy

A policy provides guidelines that regulate an agency's actions and the conduct of its people, including any necessary tasks, functions and operating parameters. A policy also includes details of who is covered, eligibility criteria, timelines and enforcement measures.[1]

An agency should document and maintain effective policies, procedures and guidelines for the governance, and the systematic identification, analysis and evaluation of corruption risk, linked to best practice advice. The policy must assist employees to understand what corruption is, their agency's attitude to corruption, and what to do if they suspect corruption. The policy should be communicated widely within the agency.

2 People

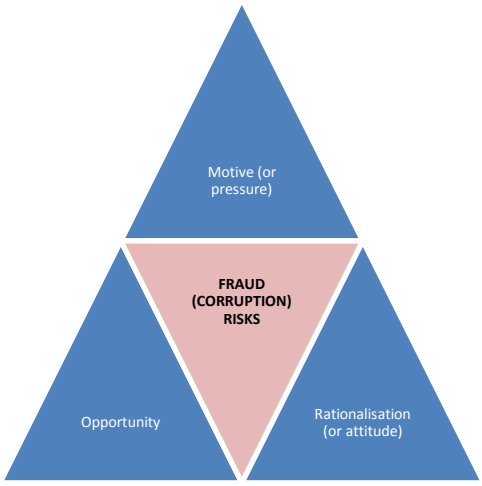
The second step involves "People". All levels of management and staff in the agency play a vital role in the corruption risk assessment process. These people must be well equipped to perform their role.

It is important that the Senior Executive Group maintain knowledge and understanding of corruption risks, and ensure that a corruption risk assessment is conducted as part of the agency's enterprise-wide risk assessment. These responsibilities can be delegated to a committee, such as an Audit and/or Risk Management Committee or a specific Fraud and Corruption Control Committee. The roles and responsibilities of the committee should be documented in a committee charter or terms of reference.

Senior executives must be committed to managing corruption risks and communicating to all employees an understanding of corruption risks and profiles, and to ensuring that these risks are recorded on the risk registers (or heat map) and treated seriously.

A fraud control officer (or risk officer), of a senior level, must lead corruption risk identification by proactive and continuing engagement with all levels of management and staff across the agency, not just senior executives. Corruption awareness and training should be delivered to all employees.

Line managers must contribute to identifying corruption risks and consider who may be in a position to commit corruption (see "The Fraud Triangle" below).



Source: adapted from *The Fraud Triangle*.

An agency's exposure to corruption is a function of the **fraud and corruption risks** inherent in their governance, culture and operations, the extent to which effective controls are present either to prevent or detect corruption, and the honesty and integrity of those involved in the process. It involves the consideration of the following three attributes.

Motive (or pressure) refers to the reason or need of the person engaged in corruption (e.g. to provide a benefit or cause a detriment).

Opportunity refers to the situation that enables corruption to occur (e.g. that controls are non-existent or inadequate to prevent or detect corruption).

Rationalisation (or attitude) refers to the mindset of the person and how they may try to justify the corruption (e.g. the honesty and integrity of those involved in the process).

[1] Campbell, NC 1998, *Effective policies and procedures: a step-by-step resource for clear communication*, American Management Association, New York, p. 10.

All employees are responsible for the prevention of corruption and contribute to identifying potential corruption risks by communicating the risks they see to their manager.

3 Process

Corruption risk assessment is a significant component of the *AS/NZS ISO 31000:2009* risk management process. It is a dynamic process consisting of three steps: [2]

- Identify risk
- Analyse risk
- Evaluate risk.

In the risk assessment process there are four layers of risk rating to be recorded in the risk registers to facilitate better decisions in mitigating the risks and, ultimately, achieving better outcomes.

The four layers of risk are:

1. Inherent risk	The risk before considering the effectiveness of existing controls. The analysis of risk involves an examination of the consequences of the corruption risks and their respective likelihoods in light of controls not in place within the agency. Inherent risk is useful in providing assistance when assessing the importance of controls and helping in the understanding of fraud and corruption penetrated test scenarios. This risk does not change during the life of the risk.
2. Residual risk	The risk after considering existing controls (that is, inherent risk and controls effectiveness). This recognises the current risk rating for each of the corruption risks. This risk is dynamic because it changes as mitigating actions are implemented, or controls are removed or deemed ineffective.
3. Expected risk	The risk after considering agreed actions that have not yet been implemented.
4. Targeted risk	The desired optimal level of risk, which should match the risk appetite of the agency.

Below is a brief overview of the corruption risk assessment process and the use of the four layers of risk rating.

Identify risk

Designing and implementing corruption risk assessment processes requires a comprehensive understanding of an agency's vulnerabilities, in both internal and external contexts. This understanding will assist all levels of management and staff in identifying and developing a listing of corruption risks (e.g. a risk register) and the sources of risk that could have an impact on the achievement of the agency's priorities. The risk identification should also consider the potential for management override of controls and the potential for collusion at the agency, significant location and business process levels. It should also consider who may be in a position to engage in corruption (that is, "The Fraud Triangle").

Analyse risk

Once known risks are established, it is necessary to analyse the consequences of those risks and their respective likelihoods, using the agency's risk analysis matrix. In this process the inherent risk rating will be calculated (e.g. low, medium or high) (*1st layer of risk*). This allows a separation of low and potential risks, and focuses attention and resources towards the highest risks for more detailed and thorough analysis.

This more detailed analysis of risk will involve the mapping of current controls and an examination of the effectiveness of those controls in managing the risks identified. At the end of the analysis, a residual risk rating is calculated in light of the effectiveness of the range of controls presented (*2nd layer of risk*).

[2] Refer to AS/NZS ISO 31000:2009: *Risk management – Principles and guidelines*.

Evaluate risk

An evaluation of the residual risk rating is undertaken to facilitate decisions on whether a risk requires mitigating action. If the residual risk is not acceptable to the agency's risk appetite, decisions need to be made about whether there are any outstanding mitigating actions that need to be implemented. If those mitigating actions were implemented, an agency can then evaluate what the expected risk rating will be (*3rd layer of risk*).

If the expected risk rating is still not acceptable, further decisions are required to identify new mitigating actions to be implemented to achieve a targeted risk rating that is acceptable (*4th layer of risk*).

Reasons for doing this audit

Departments and statutory bodies operate in a complex environment and must comply with relevant statutory governance and accountability requirements. Allegations of corruption continue to be received as persons and entities who choose to engage in corrupt conduct employ more sophisticated measures in order to avoid detection by these controls.

In 2015–16 the CCC received 2674 complaints involving 6736 separate allegations of corruption.[3] This was an increase of 12 per cent when compared to the number of complaints received in 2014–15.[4] This increase may be attributed to factors including:

- The state of an agency's ethical climate or the effectiveness of strategies to achieve the desired ethical compliance.
- The maturity of an agency's risk assessment process.
- The design of controls is inadequate to mitigate corruption risks.
- The operating controls to prevent or detect corruption are ineffective. Alternatively, controls are only partially effective, rather than fully effective, in managing the risks.
- Reduction in management focus on enforcing controls compliance and managing risks.
- Reduced staffing levels resulting in controls being circumvented.
- Deterrent measures applied are not appropriate or broadly consistent across the agency, and fail to bring about the required standards of behaviour of employees.
- The increasing use and reliance on information technology.

Source: adapted from AS 8001-2008: *Fraud and corruption control*, and the CCC's previous audits

Note. During 2016–17 the CCC received 3049 complaints involving 7898 allegations, which is an increase of 14 per cent, up 2 per cent from the preceding financial year.

Taking these factors into account, agencies must be highly risk-conscious and proactive in identifying opportunities to maximise their capacity to reduce corruption. This is best achieved through a targeted and strategic process which includes:

- Identifying serious risks.
- Identifying the source/cause of the risk and the scheme(s) under which it can occur.
- Prioritising serious corruption risks.
- Evaluating the degree of tolerance towards the risk.
- Developing mitigating actions.
- Monitoring and reporting including consideration of the changing status of the context and status of risks, ongoing effectiveness of internal controls and progression treatment.

Source: adapted from AS 8001-2008: *Fraud and corruption control*

Controlling the risk of corruption is a governance issue which must be given due attention by an agency's Senior Executive Group. Serious corruption incidents or systemic corruption within an agency is indicative of a failure by the agency's Senior Executive Group to discharge the prescribed obligations referenced below.

While it is not possible to prevent all instances of corruption, it is generally recognised that a coordinated and structured approach is the most effective way to identify and manage these risks.

[3] One complaint may consist of a number of allegations.
[4] CCC's Annual Report 2015–16.

Underpinning legislation

Section 61 of the *Financial Accountability Act 2009* requires departments and statutory bodies to establish and maintain appropriate internal controls and risk management systems.

The supporting *Financial and Performance Management Standard 2009*, at section 28, further prescribes that an agency's risk management system must provide for:

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

Audit focus

The objectives of the audit were to:

- Determine whether an agency is identifying corruption risks other than, or beyond, fraud.[5]
- Assess the effectiveness of an agency's corruption risk assessment processes in reducing the potential for corruption within and against the agency.

Scope of the audit

This audit focused on the way in which the sample of departments and statutory bodies conducted corruption risk assessment processes within their agency. It was conducted in two stages.

Selection of agencies

The first stage involved selecting the departments and statutory bodies to be included in the audit.

The CCC wanted to identify an audit sample which included both high- and medium-risk entities, agencies with low reported incidents of corruption and agencies which, based on their area of operation, may be susceptible to a variety of corruption risks. Information from the CCC's *Corruption allegations data dashboard*[6] was also considered during this selection process.

The following three departments and three statutory bodies were selected to participate:

Department	Statutory body
• Education and Training	• Seqwater
• Justice and Attorney-General	• Racing Queensland
• Communities, Child Safety and Disability Services	• WorkCover Queensland

Evaluation of corruption risk assessment process

The second stage involved reviewing the policies, procedures, guidelines and practices in place in each agency for conducting corruption risk assessments. The audit considered whether these were reasonable and linked to relevant legislation, official guidelines and best practice advice. It also included evaluating the most recent corruption risk assessment process undertaken by each agency. These are detailed further below.

Policy, people and process initiatives

Each of the six agencies completed a questionnaire prepared by the CCC, which sought information on the application of risk management principles and techniques in the assessment of the risk of corruption within the agency, including those used to coordinate/oversight the process.

---

[5] Corruption is much more prevalent and serious than common fraud incidents. The CCC will determine, where possible, if there are other genuine corruption risks that an agency should have identified, and therefore, may need to control.

[6] http://www.ccc.qld.gov.au/corruption-prevention/corruption-allegations-data-dashboard

The CCC used the responses to the questionnaire to form a preliminary view as to the presence or otherwise of a sound system of risk assessment within the agency.

The agencies also provided relevant prevention documents to support their responses to the questionnaire, including their:

Corruption prevention documents	
• Code of Conduct	• Fraud and corruption control framework
• Ethics training and awareness initiatives	• "Zero tolerance" of corruption initiatives
• Risk management framework	• Terms of reference for the oversighting committee.

Most recent risk assessment workings

The Australian Standard for Fraud and Corruption Control (AS-8001-2008) is often identified as informing best practice in controlling corruption risks within an organisation. As provided in the table below it prescribes a process of implementation, continuous monitoring and improvement across four key themes. Assessing "fraud and corruption risk" is one of the initiatives within the Australian Standard's "prevention" theme, together with the required "planning and resourcing" initiatives, to implement the identification, analysis and evaluation of corruption risks.

Our audit methodology involved a review of relevant documents, to determine whether each agency identified their corruption risks and established a plan setting out their approach to controlling their exposure to each risk.

The audit did not test the adequacy of internal controls to prevent and detect corruption, or seek to detect acts of corruption.

The highlighted areas in the following table are the extent of our audit work.

AS 8001-2008 Fraud and corruption control			
Theme 1: Planning and resourcing	**Theme 2: Prevention**	**Theme 3: Detection**	**Theme 4: Response**
A. Fraud and corruption control planning	**D.** Implementing and maintaining an integrity framework	Implementing a fraud and corruption detection program	Policies and procedures
B. Review of the fraud and corruption control policy and plan	**E.** Senior management commitment to controlling the risk of fraud and corruption	Role of the external auditor in detection of fraud	Investigation
C. Fraud and corruption control resources	Line management accountability	Avenues for reporting suspected incidents	Internal reporting and escalation
Internal audit activity in the control of fraud and corruption	Internal control	Whistle-blower protection program	Disciplinary procedures
	F. Assessing fraud and corruption risk		External reporting
	G. Communication and awareness		Civil action for recovery of losses
	Employment screening		Review of internal controls
	Supplier and customer vetting		Insurance
	Controlling the risk of corruption		

Legend:

A B C D E G	Included in scope of the audit (higher-level review)
F	Included in scope of the audit (detailed review)

Findings from the audit

Strengths

The following strengths were identified from the audit:

- A fraud and corruption control policy and/or plan is in place in each agency.
- A Code of Conduct for the Queensland Public Service, or equivalent public sector entity Code of Conduct, is in place.
- Senior executives are committed to high standards of integrity and ethical behaviour within the agency, including the management of corruption risks.
- Training and awareness on ethics, fraud and corruption is in place in each agency.
- Corruption risks are identified, analysed and evaluated through enterprise risk management.
- All agencies informally identified their top five corruption risks, which included both fraudulent and corrupt activity.

Areas for improvement

Knowing where corruption is most likely to occur is essential to managing the risk effectively. It is impossible to eliminate all corruption in an agency. Designing and implementing an effective corruption risk assessment process can be challenging, and applying its provisions effectively can also be demanding. However, design and operating effectiveness are both crucial to maximising the outcomes from corruption risk assessment processes.

Our review found that six departments and statutory bodies conducted corruption risk assessments which are linked to their risk management framework.

The audit identified the following 12 areas for improvement.

Area for improvement 1 – Define "fraud" and "corruption"

The audit identified that one of the six agencies had a fraud and corruption control plan that does not define "fraud" and "corruption". As staff are a main source of information and reporting on suspected corrupt conduct, they need to be aware of what constitutes fraud and corruption.

Recommendation

Clearly define "fraud" and "corruption" in the fraud and corruption control plan which is integral to all linked programs in delivering the agency's objective.

Note. In responding to this audit, the agency will insert definitions of "fraud" and "corruption" in the fraud and corruption control plan, and also consider including information about their anti-corruption strategies.

Area for improvement 2 – Communicate the fraud and corruption control plan widely

The audit identified that one of the six agencies only published their fraud and corruption control plan to a limited audience. The agency explained this limited circulation on the basis that the fraud and corruption control plan contains information about detection and prevention controls which if disclosed to all could counteract the intention and effectiveness of the plan.

The CCC does not consider this a valid reason for not circulating the fraud and corruption control plan more broadly. The fraud and corruption control plan is a document summarising an agency's anti-corruption strategies and may have a deterrent effect on employees who may be motivated to engage in fraud or become involved in corrupt conduct. All staff have a responsibility for controlling corruption risks; to do so, they require an understanding of the proposed strategies and current controls in place.

Recommendation

Communicate and make available the fraud and corruption control plan to all staff to assist them in managing corruption risks and reporting suspected acts of fraud and corruption. The fraud and corruption control plan could include summarised information about the agency's anti-corruption strategies.

Note. The agency acknowledged the recommendation and will work with the CCC to implement it.

Area for improvement 3 – Frequency of review of the fraud and corruption control plan

We identified one agency which only reviews their fraud and corruption control plan every five years. Its next review is scheduled for 2022.

The Australian Standard states that the fraud and corruption control plan should be reviewed and amended at intervals appropriate to the entity but, at a minimum, once every two years. Changes to an agency's operating or regulatory environment or significant technological change can impact how effective an agency's fraud and corruption control plan is in combating corruption.

Recommendation

Review the fraud and corruption control plan (including the risk assessment process) at intervals appropriate to the agency but, at a minimum, once every two years. If there is a change in the operating environment or significant technological change during the life of the fraud and corruption control plan, the plan should be reviewed immediately (i.e. without waiting the two-year review period).

Note. The agency acknowledged the recommendation and will now conduct a review of their fraud and corruption control plan once every two years, at a minimum, and more frequently if there is a change in the operating environment or significant technological change in the agency.

Area of improvement 4 – Conduct regular assessment of your agency's ethical culture

The CCC audit identified that one agency had no provision for the assessment of its ethical culture, which is a key strategy in managing the risk of fraud and corruption.

The ethical culture or behaviour of an agency's senior executives, management and staff has a general effect on risk management and internal controls across the agency. The level of risk may vary across division, business unit, process and location. For example, the level of risk relating to ethics principles and ethical values may be higher in some locations than others. Some business units may have more ethically minded staff, leading to a significant reduction in corruption risks associated with staff integrity in that business unit.

Recommendation

Conduct a regular assessment of the agency's ethical culture for:

- comparison between the various business units
- comparison of its performance over time.

This can be achieved by distributing a confidential and structured questionnaire to all staff, and collating and analysing the results.

Note. In responding to this audit, the agency has stated they will consider undertaking a questionnaire to evaluate their ethical culture in 2018.

Area for improvement 5 – Record and consider the four layers of risk rating

Our review identified that while all agencies recorded a residual risk rating (*2nd layer of risk*):

- Four out of six agencies do not record an inherent risk rating (*1st layer of risk*).

  (Note. Inherent risk may be less relevant for agencies with an established control environment and some degree of pre-existing controls. None the less, it provides agencies with an understanding of the highest corruption risks facing their business, which can assist them in better prioritising risks.)
- None of the agencies recorded an expected risk rating (*3rd layer of risk*).
- Two out of six agencies have not identified and stated their targeted risk rating (*4th layer of risk*).[7]

Residual risk rating will always be an important part of the risk assessment process. Adding the additional layers of risk rating will contribute to better evaluation and decisions about the relevant risk being considered.

Application of the four layers of risk rating will show agencies:

- The perceived effectiveness of existing controls and how much these controls help in reducing the inherent corruption risk to which they related; for example, the assurance required on existing controls.
- The importance of outstanding mitigating actions which, if implemented, will reduce the residual risk rating, should the residual risk be unacceptable to the agency.
- The extent of new mitigating actions (that is, treatments) that need to be implemented in order to reduce the likelihood and/or consequence of the related risk to the agency's risk appetite.

The four layers of risk rating assist with continual improvement to the risk assessment process, and help an agency to priorities resources, focus attention and make decisions to deal effectively with potential residual risks.

Recommendation

Record the four layers of risk in controlling corruption in risk registers. The decision should take into consideration the risk management system (to capture, link, analyse and evaluate), cost and benefit, and the usefulness of the additional layers in decision-making capabilities

Note. Agencies have acknowledged the recommendation and shown commitment to considering the value of the four layers of risk in controlling corruption.

Area for improvement 6 – Promote awareness of potential corruption risks and vulnerabilities

None of the six agencies audited document potential corruption risks in their fraud and corruption control plan. Further, five of the six agencies do not document the significant areas of their business processes that are vulnerable to fraudulent and corrupt activity.

This information, if included in the fraud and corruption control plan, will promote staff awareness of the corruption risks faced by the agency.

Recommendation

Summarise potential corruption risks and significant areas vulnerable to fraudulent and corrupt activity, as identified by the corruption risk assessment process, in the fraud and corruption control plan. Also, consider addressing this in both an internal and external context.

Note. Agencies have acknowledged the recommendation and the need to better communicate corruption risks to provide oversight on fraud and corruption risks, promote identified risks and allow a focus on prevention activities.

[7] See page 7 and the glossary of terms for the four different risk ratings.

Area for improvement 7 – Link potential corruption risks in the risk registers

We identified that three of the six agencies record potential corruption risks in their risk register at an agency level, but not at an operational level (that is, in a specific corruption risk register or operational risk registers with corruption risks flagged).

One agency had a specific risk register for potential corruption risks, but it does not always align to business areas' operational risk registers. The business areas' operational risk registers do not cover a comprehensive listing of corruption risks.

The two remaining agencies reflected their identified potential corruption risks to some extent in their risk registers.

As risk registers are a major source of information to feed into the fraud and corruption control plan and mitigating programs of an agency, failure to capture and record potential corruption risks will impact on the usefulness, relevance and quality of that plan.

Recommendation

Ensure corruption risks that are considered potentially the most damaging to the agency can be linked to divisional and/or operational risk registers (or a specific fraud and corruption risk register), as the main sources of information informing enterprise risk.

Note. Agencies acknowledged the importance of risk registers at certain levels within the organisation and will work towards enhancing their risk registers across the agency at strategic/enterprise, divisional and operational levels.

Area for improvement 8 – Enhance risk registers

The CCC audit identified that three of the six agencies have detailed fraud and corruption risk registers or operational risk registers that include more than one corruption risk. The remaining three agencies have only one broad fraud risk set out in their enterprise risk register with no comprehensive identification of corruption risks in the operational risk registers.

Recommendation

Design, implement and maintain operational risk registers for all individual operational business units that identify a comprehensive listing of potential corruption risks. Fraud and corruption risks should easily be transferred or reported at the agency level (or transferred to a specific fraud and corruption risk register that is commonly used to communicate with the Senior Executive Group, and the Audit and/or Risk Management Committee).

Note. Agencies acknowledged the recommendation and will continue to identify the best approach to ensure that various risk registers operate effectively.

Area for improvement 9 – Establish the internal and external parameters in risk assessment

The audit identified that one of the six agencies does not establish the internal and external parameters for corruption risk assessment in their process. This is an important first step to enable an understanding of the operating environment, emerging threats, culture and regulatory changes that could potentially create corruption risks to the agency.

Recommendation

That the agency establish an understanding of the external and internal contexts as they relate to corruption threats facing the agency. The context is to be documented in the fraud and corruption control plan.

Note. In responding to this audit, the agency agreed that internal and external parameters have to be established by engaging with the business units during the corruption risk assessments.

Area for improvement 10 – Establish risk appetite statements for fraud and corruption

The audit identified two agencies with no articulated risk appetite statement for "fraud and corruption" to help decision-makers determine whether a corruption risk is acceptable or tolerable, and whether action is required to ensure that a risk is treated to bring it to an acceptable or tolerable level.

A risk appetite statement for fraud and corruption is the amount of risk the agency is willing to tolerate in pursuit of reducing the incidence of corrupt conduct. A well-articulated risk appetite for the risk type of "fraud and corruption" leads to better decisions and ultimately better outcomes.

The following two case studies illustrate the importance of the concept of risk appetite.

The first case study demonstrates how every individual is prepared to take some level of risk in their personal life. In determining that level of risk, you ask and answer certain questions. The same consideration should apply within agencies when determining their appetite for corruption-related risks.

Case study: Risk appetite consideration

Ask yourself these questions:

- Would you drive a car if the seat belt was broken?
- Would you purchase a motorcycle with faulty brakes?
- Would you post a potentially compromising picture of yourself on Instagram?

Your answers to these questions will start to give you an idea of your personal risk appetite. Your personal risk appetite has a big influence on how you live your life.

In exactly the same way, your agency's appetite for certain types of risks should direct how each risk identified is to be controlled. The Senior Executive Group should establish and agree on risk appetite statements.

The second case study is an example of what a risk appetite statement may look like in an agency (note that it does not cover everything a risk appetite statement would have). It also shows that a range of appetites are applied for different types of risk category.

Case study: Risk appetite statement

Agency XYZ has a measured appetite with respect to all risk categories except compliance, safety and financial overrun, an area in which it is highly risk averse.

In delivering the Strategic Plan, the agency will take considered risks where there is a high degree of confidence that controls are in place to minimise the likelihood of adverse consequences (including preventable and unforeseen harm to customers and members of the public), and where there is a high likelihood of capturing expected and considered benefits or opportunities.

This appetite for risk affects the controls put in place to deal with it and reflects Agency XYZ's priorities (noting that it is not an exhaustive list of appetite and categories):

Appetite level	Category guide	Decision guidance
Low	Fraud	Zero tolerance for fraud or theft
Low	Legislation compliance	Strict compliance with legislative and regulatory obligations is demanded
High	Innovation	Prepared to invest for reward despite uncertainty and the possibility of some financial loss on an individual project.

As far as reasonably practicable, Agency XYZ is not willing to accept or be exposed to risk that compromises their ability to meet their obligations — these are the areas in which the agency has the lowest risk appetite.

Recommendation

Prepare risk appetite statements for different types of risk category (for example, business risk, safety risk, security risk, innovation risk and corruption risk). An agency's risk appetite for fraud and corruption is to be reflective of its shared obligation, with the CCC, to reduce the incidence of corrupt conduct in the public sector, and to achieve a zero-tolerance culture for fraud and corruption.

Note. One agency advised the CCC that they have prepared risk appetite statements for their business and these have been agreed to by the Senior Executive Group.

The other agency accepted the recommendation.

Area for improvement 11 – Prioritise and assess existing controls' effectiveness

Our review of the operational risk registers in place at each agency identified that one agency has no record of current controls in place for the related risk. It is important for current controls to be mapped to the related risk, and the assessment completed to determine the extent of controls assurance required (that is, mitigation actions).

Recommendation

Once the potential corruption risks are identified, record what controls currently exist to reduce the risk to which they relate. These controls are to be recorded in the risk register.

Note. The agency acknowledged the recommendation and will work towards addressing it.

We also identified that three of the six agencies (including the agency mentioned above) have not assessed the effectiveness of a range of existing controls against the related risk. This assessment should conclude whether the controls are, or are likely to be, effective, partially effective or ineffective, in mitigating the corruption risk to which each control relates.[8]

Recommendation

Assess the effectiveness of existing controls in managing those corruption risks. That is, whether the range of controls relating to the risk are effective, partially effective or ineffective in mitigating the corruption risk to which they relate. The assessment should be recorded in the risk register.

Note. In responding to this audit, agencies will review the effectiveness of their existing controls and the acceptability of the residual risks as they relate to fraud and corruption.

Area for improvement 12 – Reduce residual risk to the targeted risk and assign a responsible officer to manage that risk

The audit identified two agencies in which the residual risk or targeted risk was higher than the tolerable level for fraud and corruption (that is, the agency's risk appetite), as follows:

- One agency had one "High" risk, however, no targeted risk against which to measure the mitigating actions in order to bring the residual risk to the agency's lowest appetite. Further, no Risk Owner has been assigned to manage this risk.
- One agency had two "Medium" risks for which there were no proposed mitigating actions to reduce the risk to "Low". There were also outstanding actions which, if implemented, could reduce the likelihood of the risk. The agency has advised that these risks will be communicated to the Risk Owner.

Where residual risk is higher than the targeted risk, mitigating actions should be considered and implemented to reduce the risk to the desired tolerable level (that is, the risk appetite) and be assigned to a Risk Owner for actioning and monitoring.

[8] Refer to glossary of terms at the back of this report for the meaning of the three measurements of control effectiveness.

It is of primary importance that corruption risks are treated appropriately to meet the agency's risk appetite for fraud and corruption.

Recommendation

Determine if the residual risk is at an acceptable level (that is, within the agency's risk appetite). If the residual risk is not acceptable:

- First, determine what the targeted risk should ideally be. The targeted risk should equal the risk appetite or the tolerable risk. A targeted risk is to be recorded in the risk register to show the extent of mitigating actions between residual risk and targeted risk.
- Second, consider what mitigating actions are outstanding and/or implement new mitigating actions to sufficiently reduce the residual risk to the targeted risk. The response to reduce residual risk should focus on improving existing controls or implementing additional controls.

Where the residual risk is not acceptable and mitigating actions are to be implemented, assign a responsible officer to manage that potential corruption risk. The responsible officer is to be recorded in the risk register. The responsibilities for that role should already be specified in the fraud and corruption control plan.

Note. Agencies agreed with the recommendation.

Conclusion

Fraud and corruption are serious risks to the public sector and cannot be ignored. Corruption in particular is difficult to identify and has the potential to damage both an agency's operations and its reputation.

It is satisfying to see that agencies are conducting corruption risk assessments. The CCC notes, however, that fraud and corruption assessment processes within agencies could be further enhanced by implementing the recommendations outlined in the areas for improvement above.

Following the completion of our audit the CCC circulated its findings to the relevant departments and statutory bodies. Agencies acknowledged the findings and recommendations. All agencies are working towards improving their corruption risk assessment processes and practices to ensure they better identify, analyse and evaluate fraud and corruption risks, and better communicate these risks so they can be controlled effectively.

Agencies should identify a comprehensive list of fraud and corruption risks for each business process by conducting "risk storm" workshops across the agency. Risks should be carefully analysed and evaluated to identify vulnerabilities within the agency, enabling better decisions and ultimately better outcomes in the management of corruption risks.

Note

On 1 July 2017, the Australian National Audit Office withdrew most of its Better Practice Guides in favour of similar guides prepared by other Government regulators and policy owners.

One of the Better Practices Guide that has been withdrawn is "Fraud Control in Australian Government Entities".

The CCC understands that this Better Practice Guide may provide much of the basis for agencies' fraud and corruption control frameworks. If this is the case, it is recommended that each agency consider the impact on its existing framework of the withdrawal of the guide and work towards other better practices advice.

Glossary of terms (risk management)

Control effectiveness	In the context of corruption risk, an effective control is one that is considered to be effective in preventing or detecting corruption and therefore contributes to enabling the agency to achieve its overall goals and objectives. [as adapted from the Australian Standard and HB 158-2006]
Control ineffectiveness	An internal control which, by reason of its not operating as intended or some other factor, is making little or no contribution to mitigating the corruption risk under consideration and therefore makes little or no contribution towards the agency's achievement of its business goals and objectives. [as adapted from the Australian Standard and HB 158-2006]
Control partially effective	An internal control which, by reason of its not operating as intended or due to some other factor, is not fully effective in managing the risk it is intended to manage but is making some contribution towards managing the corruption risk under consideration and therefore makes some contribution towards the agency meeting its goals and objectives. [as adapted from the Australian Standard and HB 158-2006]
Expected risk	The risk after considering agreed actions that have not yet been implemented (*3rd layer of risk*).
Inherent risk	The risk that is a consequence of an agency's business, and before considering existing controls (*1st layer of risk*).
Internal control	The Committee of Sponsoring Organisations (COSO) defines internal control as "a process, effected by an entity's management, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance". For example, the policy, people and process of an entity designed to help it mitigate a risk and achieve specific goals or objectives.
Mitigating actions	Agreed mitigating actions to further treat risk.
Residual risk	The risk remaining after factoring the inherent risk and control effectiveness rating (*2nd layer of risk*).
Risk appetite	The amount of risk that the agency is prepared to accept or be exposed to at any point in time. Also, known as the targeted risk.
Targeted risk	The desired optimal level of risk (equates to the risk appetite) (*4th layer of risk*).

References

Cressey, Donald R., *Other People's Money*, "The Fraud Triangle", Montclair: Patterson Smith (p. 30), 1973.

SAI Global, *Risk Management – Principles and Guidelines*, SAI Global, Sydney, 2010.

SAI Global, *Fraud and Corruption Control*, SAI Global, Sydney, 2008.

Crime and Corruption Commission
QUEENSLAND

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace, Fortitude Valley QLD 4006

Phone: 07 3360 6060
(toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

www.ccc.qld.gov.au

Stay up to date

Subscribe for news and announcements:
www.ccc.qld.gov.au/subscribe

Follow us on Twitter:
@CCC_QLD