

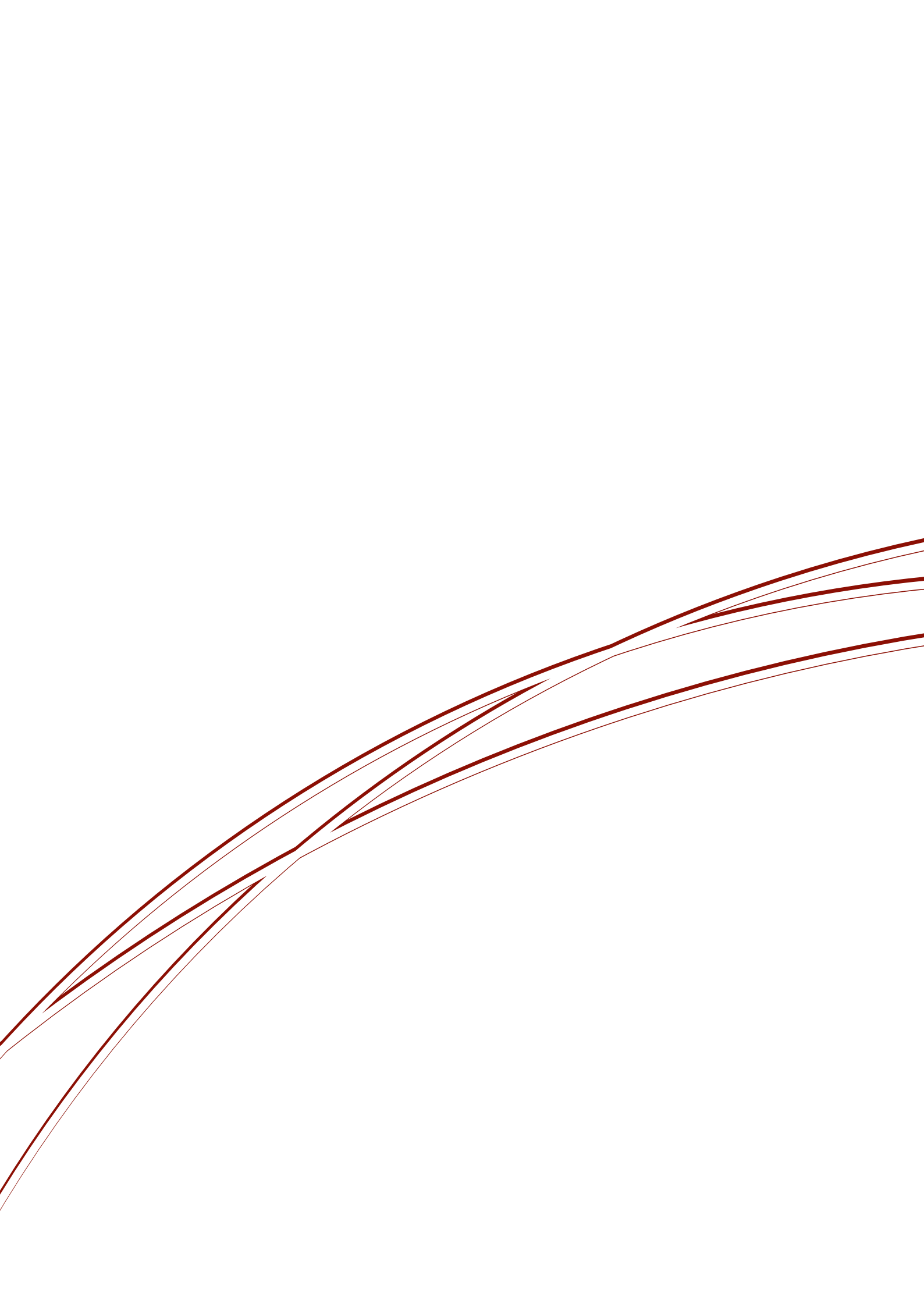


INDEPENDENT COMMISSION  
AGAINST CORRUPTION  
NEW SOUTH WALES

Maturity level	Period	Information to
Low	Low	<ul style="list-style-type: none"><li>Information about corruption vulnerabilities is provided on request.</li></ul>
Medium	Medium	<ul style="list-style-type: none"><li>As per Low</li><li>Routine provision of information about corruption vulnerabilities to specific Line 1 functions.</li></ul>
High	High	<ul style="list-style-type: none"><li>As per Medium, but effort to tailor information to managers.</li><li>Planned program to identify gaps in understanding vulnerabilities.</li></ul>

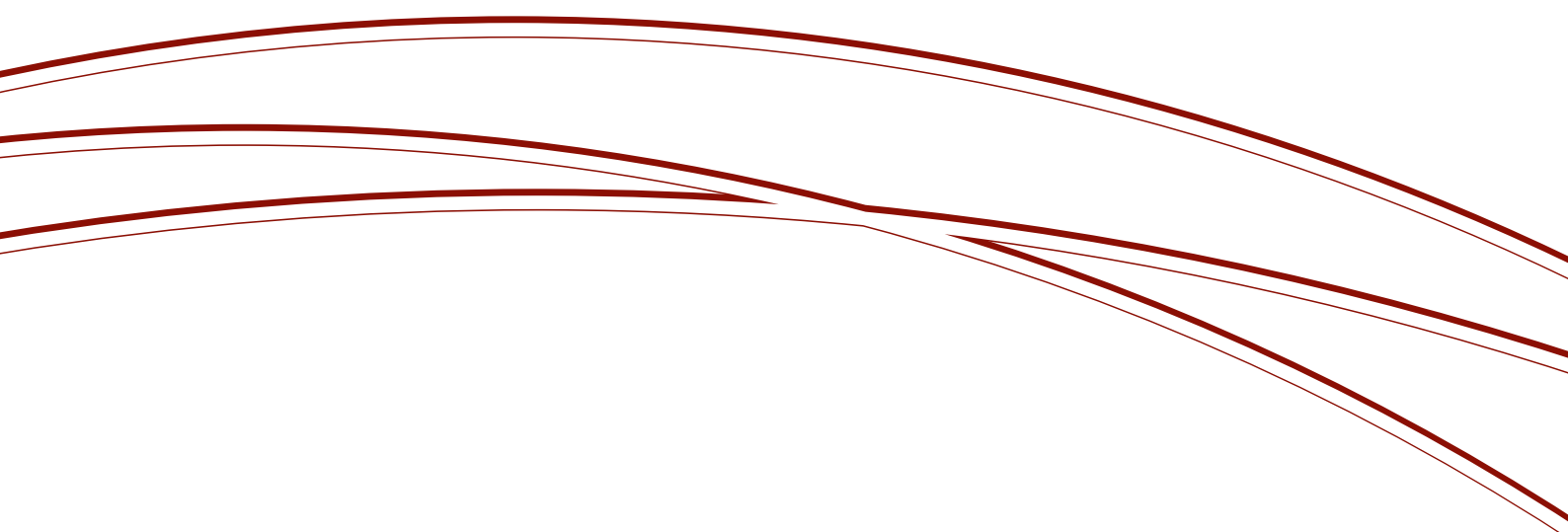
# ASSESSING CORRUPTION CONTROL MATURITY

FEBRUARY 2023





INDEPENDENT COMMISSION  
AGAINST CORRUPTION  
NEW SOUTH WALES



---

## ASSESSING CORRUPTION CONTROL MATURITY

---

**February 2023**

---

© February 2023 – Copyright in this work is held by the Independent Commission Against Corruption. Division 3 of the *Copyright Act 1968* (Cwlth) recognises that limited further use of this material can occur for the purposes of “fair dealing”, for example study, research or criticism, etc. However if you wish to make use of this material other than as permitted by the Copyright Act, please write to the Commission at GPO Box 500 Sydney NSW 2001.

ISBN: 978-1-922581-03-7

This publication and further information about the Independent Commission Against Corruption can be found on the Commission’s website at [www.icac.nsw.gov.au](http://www.icac.nsw.gov.au).

Public sector organisations are welcome to refer to this publication in their own publications. References to and all quotations from this publication must be fully referenced.



INDEPENDENT COMMISSION  
AGAINST CORRUPTION  
NEW SOUTH WALES

Level 7, 255 Elizabeth Street  
Sydney NSW 2000 Australia

**Postal address:** GPO Box 500  
Sydney NSW 2001 Australia

**T:** 02 8281 5999

**Toll free:** 1800 463 909 (for callers outside metropolitan Sydney)  
National Relay Service users: ask for 02 8281 5999

**F:** 02 9264 5364

**E:** [icac@icac.nsw.gov.au](mailto:icac@icac.nsw.gov.au)

**[www.icac.nsw.gov.au](http://www.icac.nsw.gov.au)**

**Business hours:** 9 am to 5 pm, Monday to Friday

# Contents

<b>Chapter 1: Introduction</b>	<b>5</b>	Protecting vulnerable systems and processes	22
The need for a better practice publication	5	Process and system design	24
How to use this publication	6	Relevant Australian Standard sections	25
Definitions used in this publication	6		
<b>Chapter 2: Overview of better practice corruption control</b>	<b>8</b>	<b>Chapter 5: Detecting corrupt conduct</b>	<b>26</b>
		Complaint mechanisms	26
<b>Chapter 3: Building integrity</b>	<b>12</b>	Review and analysis mechanisms	29
Promoting integrity	12	Relevant Australian Standard sections	30
Integrity is promoted via a range of techniques and forums	14	<b>Chapter 6: Responding to integrity breaches</b>	<b>32</b>
An organisational environment that fosters integrity	14	Responding to specific breaches	32
Stopping unethical actors	17	Patterns of breaches	36
Relevant Australian Standard sections	18	Informing corruption control efforts	36
		Relevant Australian Standard sections	37
<b>Chapter 4: Preventing corrupt conduct</b>	<b>19</b>	<b>Chapter 7: Corruption risk management</b>	<b>38</b>
Enhancing organisational performance	19	Integration with agency business	38
Developing the integrity policy framework	19	Robustness of corruption risk analysis	39
Identifying corruption vulnerabilities	21		

Effective and efficient corruption controls	41
Relevant Australian Standard sections	43

<b>Chapter 8: Corruption control framework</b>	<b>44</b>
--	-----------

Framework features	44
Corruption control plan	46
Relevant Australian Standard sections	47

<b>Chapter 9: Corruption control roles</b>	<b>48</b>
--	-----------

Generalist staff	48
Specialist functions	48
Senior management accountabilities	50
Audit and risk committee	50
Relevant Australian Standard sections	52

<b>Chapter 10: Corruption control competence</b>	<b>54</b>
--	-----------

Generalists	54
Corruption control specialists	58
Relevant Australian Standard sections	59

# Chapter 1: Introduction

NSW public sector agencies face a variety of corruption risks. While it is challenging to manage these risks effectively and efficiently, the challenge is reduced if an agency establishes a robust corruption control program. This publication provides guidance to NSW public sector agencies on better practice corruption control to help them establish such a program.

Under s 13(2)(c) of the *Independent Commission Against Corruption Act 1988* (“the ICAC Act”), the NSW Independent Commission Against Corruption (“the Commission”) conducts its investigations with a view to determining “whether any methods of work, practices or procedures of any public authority or public official did or could allow, encourage or cause the occurrence of corrupt conduct”.

As a result, Commission investigation reports usually make observations about deficiencies in systems and processes that may be conducive to corrupt conduct. While some deficiencies are easily addressed, more frequently they indicate a broader failure in an agency’s approach to corruption control. For instance, deficiencies regarding organisational performance management, risk management and assurance are perennially identified as corruption prevention issues in Commission investigations.

This publication equips agencies with the means to answer two key questions:

- How robust are their corruption control systems and processes?
- How do they organise and coordinate their corruption control efforts?

## The need for a better practice publication

A need to systematise corruption control efforts is clearly prescribed in the NSW Government *Fraud and Corruption Control Policy* (Treasury Circular TC18-02), which requires all NSW State Government agencies (including State Owned Corporations) to “...develop, implement and maintain a fraud and corruption control framework to prevent, detect and manage fraud and corruption”. Similarly, the NSW Office of Local Government states that “Councils should have a fraud and corruption control framework which identifies and manages the risk of incidence of fraud or corruption and includes prevention and monitoring strategies”.<sup>1</sup>

As part of the background research conducted for this publication, the Commission consulted with and/or reviewed publications provided by sources such as:

- other anti-corruption and integrity agencies
- private sector, government and non-government organisations with expertise in corruption control
- corruption control specialists
- relevant standards, guidelines and related documents
- academic research
- the Commission’s data holdings.

This research highlighted that while there is considerable guidance available regarding distinct elements of corruption control, there was no document that provided a detailed

<sup>1</sup> [Fraud and Corruption Prevention](#) - Office of Local Government NSW; Accessed 2 May 2022.



overview of what a better practice corruption control framework looks like for NSW public sector agencies.<sup>2</sup>

## How to use this publication

The focus of this publication is on *improving* corruption control. It has been designed so that agencies can assess their corruption control systems and processes, and then map their strengths and weaknesses. This publication provides descriptions of different “maturity levels” for each feature. Maturity levels are the level that an agency has reached in managing its corruption vulnerabilities. They are categorised as Low, Medium and High, and are demonstrated via tables included throughout this publication. These descriptions also facilitate an understanding of the outcomes.

While the Commission encourages agencies to test themselves against this publication, it is neither a standard or a compliance document, and does not seek to replace such documents. Also, while it indicates *what* high maturity looks like, it does not provide detailed guidance about *how* high maturity can be achieved. For this reason:

- chapters 3–10 each list relevant sections from the Australian Standard on Fraud and corruption control (AS8001:2021)
- the Commission will list additional resources for each chapter on its website.

Additionally, the Commission does not expect agencies to be at the High maturity level for every feature at any point in time. This is because all agencies face challenges to establishing and maintaining better practice corruption control due to factors such as:

- public sector complexity and machinery of government changes
- resource limitations and staff turnover
- ongoing changes in the corruption risk environment.

This publication provides information that should allow any agency to improve its corruption control systems and processes regardless of its maturity level.

Where possible, different maturity levels are described in terms of outcomes. This is because the Commission

persistently finds cases where control systems appear robust on paper but are poorly implemented in practice. An agency using this publication needs to properly assess whether these outcomes have been achieved or risk creating a false sense of security.

## Definitions used in this publication

**Assurance:** Any activity conducted with the aim of ensuring that activities conducted by an agency or on its behalf occur as prescribed.

**Corrupt conduct:** (As defined in s 7, s 8 and s 9 of the ICAC Act). For the purposes of this publication, the terms “corrupt conduct” or “corruption” are used interchangeably. In addition, under the ICAC Act, fraud by a public official or affecting a public sector agency falls within the definition of corrupt conduct.

**Corruption control:** The minimisation of the effects of corrupt conduct. This can involve preventing, otherwise lowering the likelihood of, or reducing the consequences of corrupt conduct.

**Corruption risk management:** The process by which corruption risks are identified, assessed and managed. It may focus solely on corruption risks or also include other categories of risk.

**Hard controls:** Formal controls such as policies and procedures, managerial sign-off and review, documented plans and segregations of duties.

**Integrity:** Behaviour that aims to ensure that the right thing is done. In an organisational context, the “right thing” includes both the fulfilment of an agency’s objectives, and simultaneously upholding ethical, behavioural and professional standards.

**Integrity breach:** An action taken by an entity with respect to an agency that transgresses its ethical, behavioural or professional standards. Corrupt conduct is a type of integrity breach.

**Organisational associates:** Any entity that is not staff but nevertheless contributes to an agency’s activities (for example, a supplier, partner or regulated entity).

**Soft controls:** Informal controls such as competency, staff knowledge and understanding, ethical behavioural norms and relationship building.

**Staff:** One or more individuals who provide labour for an organisation, including employees and individual contractors.

<sup>2</sup> The Australian Standard on *Fraud and Corruption Control* (AS 8001:2021) provides some useful guidance but it is not specifically written for NSW public sector agencies. In addition, the Audit Office of NSW *Fraud Control Improvement Kit*, last issued in 2015, is no longer being maintained. The Commission has worked closely with the Audit Office to produce this publication, which seeks to continue the key messages contained in the kit.



### **Three lines of defence model/Three lines model:**

A framework for the implementation of assurance that categorises activities into the following three “lines”:

- **Line 1:** Activities performed by operational managers and staff (that is, risk owners)
- **Line 2:** Activities performed by specialist risk management, governance or compliance functions (for example, corruption control activities performed by corruption control specialists)
- **Line 3:** Activities performed by an agency’s internal audit function. It should be noted that some organisations regard external audit, and the audit and risk committee, as part of Line 3.

## Chapter 2: Overview of better practice corruption control

This chapter provides an overview of the Commission's understanding of better practice corruption control, which provides a snapshot of the corruption control maturity elements and outcomes discussed in chapters 3–10.

This has been done to:

- provide a summary of the content in chapters 3–10
- allow readers who are interested in specific content to readily identify where in the publication that content is discussed in detail
- fill the void, noted in chapter 1, of a holistic description of better practice corruption control.

Better practice corruption control is built on four key pillars of control:

- Building integrity
- Preventing corrupt conduct
- Detecting corrupt conduct
- Responding to integrity breaches

and four supporting systems and processes:

- Corruption risk management
- Corruption control framework
- Corruption control roles
- Corruption control competence.

### Building integrity

As discussed in chapter 3, this pillar refers to controls designed to ensure that integrity is a key feature of the agency, and that its organisational environment results in staff behaving with integrity by default.

First, integrity is systematically promoted to staff and organisational associates in a manner that:

- links integrity to organisational success
- promotes integrity via a range of techniques and in a variety of forums.

Secondly, the organisational environment fosters integrity by ensuring that:

- integrity is incentivised
- the organisational culture supports integrity.

Thirdly, the agency stops unethical actors by:

- systematically conducting due diligence screening
- not tolerating integrity breaches.

### Preventing corrupt conduct

As discussed in chapter 4, this pillar refers to controls designed to ensure that organisational systems and processes make it challenging to engage in corrupt conduct.

First, organisational performance is robustly managed.

Secondly, in relation to an agency's integrity policy framework:

- the framework has sufficient coverage of integrity issues to clearly articulate relevant requirements
- integrity policies are communicated in a manner that ensures these requirements are understood
- the agency ensures compliance with these requirements.

Thirdly, the agency ensures that:

- frontline managers use their understanding of corruption risk to identify vulnerabilities
- specialist corruption control units continually update and share their understanding of corruption vulnerabilities
- an independent internal audit unit identifies corruption vulnerabilities as part of its work.

Fourthly, the agency takes additional steps to protect systems that are simultaneously vulnerable and widely used within the agency, namely:

- applying more stringent controls to high-risk processes and systems
- monitoring the residual corruption risk
- taking timely and appropriate action in response to audit and review findings.

Fifthly, when designing processes and systems:

- segregations of duties are considered and enforced
- clear accountabilities are set
- reliable information is readily available to someone overseeing or reviewing the process.

## Detecting corrupt conduct

As discussed in chapter 5, this pillar refers to controls designed to ensure that any corrupt conduct that occurs is detected quickly.

First, the agency effectively manages complaints of wrongdoing by ensuring that:

- a documented process is in place

- complainants find it easy to make a complaint
- the agency demonstrates that it genuinely values complaints
- complaint handling processes manage relevant risks.

Secondly, the agency adopts a variety of review and analysis mechanisms to identify potential corrupt conduct, namely that:

- the frontline routinely checks for red flags of corrupt conduct and organisational systems support the review of these red flags
- assurance units adopt a range of additional measures to identify potential corrupt conduct.

## Responding to integrity breaches

As discussed in chapter 6, this pillar refers to controls designed to ensure the agency responds to integrity breaches in a comprehensive but proportionate manner.

First, the agency responds to specific integrity breaches in a manner that demonstrates that “something will be done”, namely that:

- alleged integrity breaches constituting corrupt conduct or other serious misconduct are appropriately reported externally by agencies and investigated
- proportionate action is taken in response to established integrity breaches.

Secondly, the agency systematically analyses patterns of integrity breaches.

Thirdly, insights from integrity breaches inform an agency’s corruption control program.

## Corruption risk management

As discussed in chapter 7, better practice corruption control is supported by the robust management of specific corruption risks.

First, corruption risk management is integrated with organisational business in that:

- managing corruption risk is treated as a routine part of an agency's operations
- it occurs at strategic, operational and project levels
- it occurs during both planning and development, and operations phases
- the ownership of corruption risks and controls is located across the agency with corruption control specialists playing a coordinating role.

Secondly, corruption risk analysis is sufficiently robust in that:

- corruption risks are analysed using appropriate methodology, standards and approaches
- an agency's operating environment informs its analysis of corruption risks
- corruption risk analysis is performed with sufficient frequency across the organisation to ensure that an agency's knowledge of its corruption risk profile is current
- when analysing corruption risks, it is explicitly considered that corruption risks may manifest differently across the agency.

Thirdly, in relation to an agency's corruption controls:

- a sufficiently broad range of controls is used
- the application and evaluation of controls supports agency outcomes.

## Corruption control framework

As discussed in chapter 8, better practice entails a robust corruption control framework ("Framework"), which includes a corruption control plan or strategy ("Plan").

First, the Framework is robust in that it is:

- rigorous from a corruption control perspective
- ensures that corruption control activity is adapted to an agency's internal context.

Secondly, the Plan that is part of the Framework efficiently and effectively coordinates corruption control activity in that it:

- provides a detailed description of an agency's corruption control efforts
- is tailored to the agency's operational environment.

## Corruption control roles

As discussed in chapter 9, better practice corruption control is supported by the careful assignment of responsibilities and accountabilities across all three lines of defence.

First, general corruption control responsibilities are assigned across the whole agency, so that all:

- staff are responsible for reporting corrupt conduct, and identifying corruption risks and control weaknesses
- managers are responsible for adopting controls to manage corruption risk within their remit.

Secondly, additional responsibilities are assigned to officers in specialist functions to ensure that:

- there are clear responsibilities for reporting against the Framework
- expert input informs the control of vulnerable processes
- corruption controls are designed and implemented effectively and efficiently.

Thirdly, senior management is assigned accountabilities to ensure that:

- corruption control activities receive sufficient organisational support and resourcing
- corruption control is integrated with other organisational activity
- senior management can readily hold an individual accountable for the agency's corruption control program.

Fourthly, the audit and risk committee ("the ARC") obtains assurance that:

- the agency's Framework represents better practice
- corruption control functions are performed in accordance with better practice
- activities of other governance functions (for example, internal audit, risk management) sufficiently consider potential corrupt conduct.

## Corruption control competence

As discussed in chapter 10, corruption control is enhanced if staff and organisational associates hold certain competencies.

First, generalist staff and organisational associates:

- have sufficient knowledge of corruption-control-related policies to ensure that ignorance is not a valid excuse for not following them
- have the ability to identify likely corruption risks and prudent control strategies
- know how to respond to suspected corrupt conduct.

Secondly, corruption control specialists:

- ensure that corruption control activity is based on input from both corruption control and process experts
- use psychological understanding of the causes of corrupt behaviour and its mitigation to inform corruption control activity
- use performance and benchmarking data to guide and monitor corruption control activity
- have the capacity to diagnose and remedy corruption control weaknesses.

## Chapter 3: Building integrity

In a democracy, government exists to serve the people. The public entrusts, and prescribes a duty on, public officials to act in the public interest. Indeed, these officials are sometimes termed public *servants*, emphasising the fact that their functions are executed for public benefit. Therefore, integrity<sup>3</sup> is a cornerstone of good government.

As noted in chapter 1, organisational integrity involves fulfilling an agency's objectives while upholding ethical, behavioural and professional standards. A lack of focus on agency objectives may result in an agency "doing the wrong thing in the right way". By contrast, a failure to ensure adherence to relevant standards might result in it "doing the right thing in the wrong way".

Those involved in the governance of an agency, including ARCs, now view integrity as a key ingredient of the control environment within the domain of "soft controls". Integrity is a key contributor to high performance, and supports the efficient and effective operation of formal (hard) controls.

Corruption control activities that build integrity aim to ensure that it is an important feature of all activities. In such an environment, staff and organisational associates behave with integrity by default. That is, ethical conduct becomes a behavioural norm.

This reduces the likelihood of corrupt conduct occurring because a culture of integrity can reduce corrupt conduct even if exploitable control weaknesses are present. Equally, prevailing norms can reduce tolerance for observed misconduct and red flags.

One hallmark of integrity is a positive reporting culture where staff are aware that they can make reports without fear of criticism or reprisal. Building integrity also

requires staff to feel confident that their reports will be appropriately assessed, handled, and investigated, including that any necessary corrective action will be taken. Internal reporting and complaint management are briefly mentioned in this chapter but are discussed in detail in chapters 5 and 6.

Three types of measures that aim to build integrity are those that:

- increase the integrity of staff and organisational associates by systematically promoting integrity
- ensure that the agency has an operational environment that supports integrity
- stop low integrity actors from undermining integrity within the agency.

### Promoting integrity

An individual's inclination to act with integrity changes over time and often depends on the situation. For instance, an officer with an unblemished record may engage in fraud if they experience unexpected financial distress.

While agencies have little control over the personal circumstances of their staff, a genuine, demonstrable commitment to acting with integrity can shape conduct. Individuals may be motivated to act ethically because of factors such as wanting to be part of a high-performance organisation, wanting to work in an agile and innovative environment, loyalty to the agency, wanting to "fit in" with co-workers, a desire for advancement or simply wanting to avoid losing their current role.

Key outcomes are that integrity is:

- linked to agency success
- promoted via a range of techniques and forums.

<sup>3</sup> Integrity, as defined in this publication, incorporates both individual and organisational ethics.

## Linking integrity messaging to agency success

One weakness that the Commission repeatedly observes is that integrity is treated as something unrelated to an agency's overall purpose. This is often compounded if the agency takes no steps to measure or benchmark integrity-related performance.

In fact, fostering workplace integrity goes hand in hand with the achievement of agency outcomes including merit-based decision-making, staff morale, employee retention and efficiency. Consequently, better practice corruption control aims to ensure that the link between integrity and high performance is well understood.

Table 1 presents these features of integrity messaging for typical cases of Low, Medium and High corruption control maturity.

**Table 1: Features of integrity messaging**

Maturity level	Performance and purpose	Messengers and cascading
<b>Low</b>	<ul style="list-style-type: none"><li>Integrity is promoted as something to strive for, but simply listed as one of a series of aims to simultaneously achieve (for example, "We strive to achieve good customer service and value for money, and act with integrity.").</li></ul>	<ul style="list-style-type: none"><li>Usually comes from Line 2 specialists<sup>4</sup>, such as corruption control and ethics managers.</li><li>Messages are rarely cascaded, usually only by particularly interested individuals.</li></ul>
<b>Medium</b>	<ul style="list-style-type: none"><li>Integrity is linked to agency financial performance and related concepts such as value for money.</li><li>May also be linked to relevant, non-financial agency risks such as under-delivery and reputational damage.</li></ul>	<ul style="list-style-type: none"><li>Integrity messaging comes from senior management.</li><li>Senior management requests that messages be cascaded.</li></ul>
<b>High</b>	<ul style="list-style-type: none"><li>Integrity is linked to agency purpose and presented as a driver of high performance. For instance, by supporting the achievement of outcomes, managing relevant risks and building trust.</li><li>Integrity messaging promotes and encourages a speak-up culture.</li></ul>	<ul style="list-style-type: none"><li>As per Medium.</li><li>Line 2 specialists advise senior management on message content and delivery.</li><li>Messages are effectively cascaded so that they are understood and discussed at all levels.</li></ul>

<sup>4</sup> The three lines of defence/three lines model is defined in chapter 1.



## Integrity is promoted via a range of techniques and forums

Different people absorb and value information in different ways. For instance, some pay particular attention to formal rules and documents, while others are more likely to listen to communication from respected colleagues. Similarly, some may prefer to learn via presentations at formal meetings whereas others may learn from watching the behaviour of senior leaders – this may include what is *not* said or done, as well as what is.

Consequently, communication approaches that do not allow for different preferences may only impact certain staff or organisational associates.

Effective promotion of integrity, therefore, requires multiple communication channels. In addition to catering for differences in how individuals absorb information, a degree of repetition helps reinforce the importance of the message.

More sophisticated approaches factor in psychological aspects that may increase likelihood of a message being comprehended and accepted. This is sometimes known as “behavioural insights” and, as an example, can involve the use of “nudges” to encourage people to act ethically. For instance, staff may be nudged to act ethically if presented with statistics indicating that the vast majority of their colleagues comply with relevant policies.

Informal channels may be as important, if not more important, to promoting integrity as formal channels. Having leaders model the desired behaviour sends a powerful signal that the agency values integrity, which also helps reinforce formal integrity messaging.

Table 2, on page 15, presents integrity promotion approaches for typical cases of Low, Medium and High corruption control maturity.

## An organisational environment that fosters integrity

An agency’s formal management and governance systems are only part of its control framework, and softer control elements can also influence employee behaviour. Indeed, in many situations, informal day-to-day cues are more likely to determine behaviour than documented policies and procedures.

Key outcomes are that:

- integrity is incentivised

- the organisational culture supports integrity.

## Integrity is incentivised

Integrity violations may be encouraged if management urges staff to “just get the job done”. That is, to prioritise ends over means. Improper incentives do not necessarily have to take the form of spoken directives. For example, merely setting an inflexible, unrealistic project deadline could give staff a reason to cut corners.<sup>5</sup>

Problems also arise when ethical conduct is ignored or criticised. This can include when an individual is punished for pointing out mistakes or red flags.

Staff performance management processes also play a role in incentivising integrity. This can involve simply rewarding individual acts of integrity, but can also include developing integrity-based key performance indicators (KPIs) and using them in performance evaluation processes. Examples include responding appropriately to public interest disclosures, completing integrity-related declarations (such as conflicts of interest, or gifts), completing required ethical training, and ensuring that subordinates meet similar ethical expectations.

Table 3, on page 16, presents how integrity is incentivised by means other than punishing integrity violations for typical cases of Low, Medium and High corruption control maturity.

## The organisational culture supports integrity

An agency’s way of doing things in practice may not correspond to its formal policies and procedures or the dictates of senior management. This can lead to a scenario where the agency’s documentation advocates for integrity but no one within the agency listens, leading to a low integrity environment.

Better practice involves both monitoring the culture and intervening to ensure that it continues to be positive. It should be noted that a single, uniform culture is unlikely for all but very small agencies, meaning that there will likely need to be a degree of granularity regarding how it is monitored.

A detailed discussion of organisational culture is beyond the scope of this publication. While there are many organisational culture elements that support integrity, four key aspects are discussed on page 16.

<sup>5</sup> This does not mean that managers are restricted from acting with a sense of urgency. Better practice process design includes alternative processes that can be used in times of urgency, together with clear and appropriate approval requirements.

**Table 2: Means of promoting integrity**

Maturity level	Messaging to staff	Messaging to organisational associates	Informal means of promotion
<b>Low</b>	<ul style="list-style-type: none"> <li>Integrity requirements are listed in agency policy documents.</li> <li>Staff receive a copy of the code of conduct when hired.</li> <li>Staff receive generic code of conduct training (or similar).</li> </ul>	<ul style="list-style-type: none"> <li>Generic statement that the agency expects organisational associates to act with integrity.</li> </ul>	<ul style="list-style-type: none"> <li>No conscious attempt by leaders to model integrity.</li> <li>Minimal attempt to integrate integrity into culture and practice of agency.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Staff certify that they will comply with the code of conduct when they are hired.</li> <li>Multiple integrity training modules exist.</li> <li>Some corporate communications promoting integrity exist.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>There are contractual obligations to act with integrity.</li> <li>Documents such as a statement of business ethics are provided to organisational associates.</li> </ul>	<ul style="list-style-type: none"> <li>Leaders make effort to avoid behaviour that could be perceived as lacking integrity.</li> <li>Integrity is discussed in forums such as team meetings (for example, “integrity moments”).</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Staff regularly re-certify that they will comply with the code of conduct.</li> <li>Integrity is discussed in the context of other training (for example, a procurement module discusses relevant integrity issues).</li> <li>Corporate communications specifically promote integrity and demonstrate that integrity breaches will be acted upon.<sup>6</sup></li> <li>Integrity messaging uses behavioural techniques (for example, nudges) where appropriate.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Ethical expectations are communicated in contexts such as briefing sessions.</li> <li>Training on ethical issues is provided on a risk-basis (for example, training is likely provided to employees of critical suppliers).</li> </ul>	<ul style="list-style-type: none"> <li>Leaders model and explain ethical behaviour.</li> <li>Integrity is considered a part of doing business, and consequently discussed in a diverse range of forums and built into decision-making processes.</li> <li>Leaders understand the psychological drivers of misconduct and can anticipate vulnerable situations.</li> </ul>

<sup>6</sup> See also chapter 6.

**Table 3: How integrity is incentivised**

Maturity level	Response to bad news	Organisational performance measures	Integrity performance management
<b>Low</b>	<ul style="list-style-type: none"> <li>Tendency to avoid criticism and “shoot the messenger” when bad news is received.</li> <li>Unpleasant discussions (including those with organisational associates) are usually avoided.</li> </ul>	<ul style="list-style-type: none"> <li>Performance measures are generally unrealistic and/or rely on an overly-narrow conception of performance.</li> </ul>	<ul style="list-style-type: none"> <li>Integrity-based KPIs either do not exist or only exist for Line 2 integrity specialists.</li> <li>Failure to reward behaviour that displays integrity.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Receipt of criticism and other bad news is tolerated, although it may be actioned inconsistently.</li> <li>Unpleasant discussions about conduct are sometimes held.</li> </ul>	<ul style="list-style-type: none"> <li>Key organisational performance measures are usually relevant and realistic, perhaps being based on a framework such as SMART (Specific, Measurable, Assignable, Realistic and Time-related).</li> </ul>	<ul style="list-style-type: none"> <li>Integrity-based KPIs exist, possibly only for relatively senior staff, but are generally vague and hard to measure.</li> <li>While there may be things like integrity awards, integrity generally is not included in performance monitoring and evaluation.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>Receipt of criticism and other bad news is accepted as an important way of improving agency outcomes.</li> <li>Bad news is transmitted as quickly as possible to the right level</li> <li>It is normal to hold unpleasant discussions about conduct.</li> </ul>	<ul style="list-style-type: none"> <li>A framework such as SMART is used to develop performance metrics across the agency.</li> <li>Periodic review is conducted to ensure that assumptions behind the metric are still valid.</li> <li>Management considers how KPIs could be gamed, manipulated or drive the wrong behaviour.</li> </ul>	<ul style="list-style-type: none"> <li>Integrity-based KPIs exist across roles of all seniority, and are clear and measurable.</li> <li>Integrity is built into performance evaluation and monitoring processes.</li> </ul>

First, integrity is a part of how the agency does business. This includes integrity being factored into organisational decision-making, the agency ensuring that it acts with integrity and influential agency staff being designated sources of integrity expertise.

Secondly, the agency has a high-performance culture (given that integrity and performance are linked). This includes high performance being promoted by all levels of management, performance being systematically operationalised and measured, and poor performance being consistently remediated.

Thirdly, the agency values continuous improvement (given this increases the likelihood of appropriate responses to

raised integrity issues). This includes the agency having dedicated review processes that result in improvements to systems and processes, and staff being encouraged to identify potential improvements.

Fourthly, there is a positive reporting culture within the agency, where reports are encouraged and staff supported. This is discussed in chapter 5.

## Stopping unethical actors

As noted above, misconduct is often driven by situational factors. Because of this, preventing corrupt conduct is not simply a case of finding the “bad apples”. That being said, Commission investigations have repeatedly identified cases where red flags of low integrity were not detected or actioned. They also indicate that individuals with a track record of misconduct are more likely to continue their behaviour unless stopped, and such individuals can facilitate a low-integrity culture.

Key outcomes are that:

- due diligence screening is systematically conducted
- integrity breaches are not tolerated.

## Due diligence screening is systematically conducted

Better practice corruption control involves the agency systematically conducting due diligence on the entities with which it deals. Such checks are made on both staff (for example, employment screening) and organisational associates (for example, supplier due diligence).

The Commission has published guidance on both employment screening and supplier due diligence<sup>7</sup> because its investigations have repeatedly identified failures in due diligence being associated with corrupt conduct.

Table 4 presents how agencies conduct due diligence for typical cases of Low, Medium and High corruption control maturity.

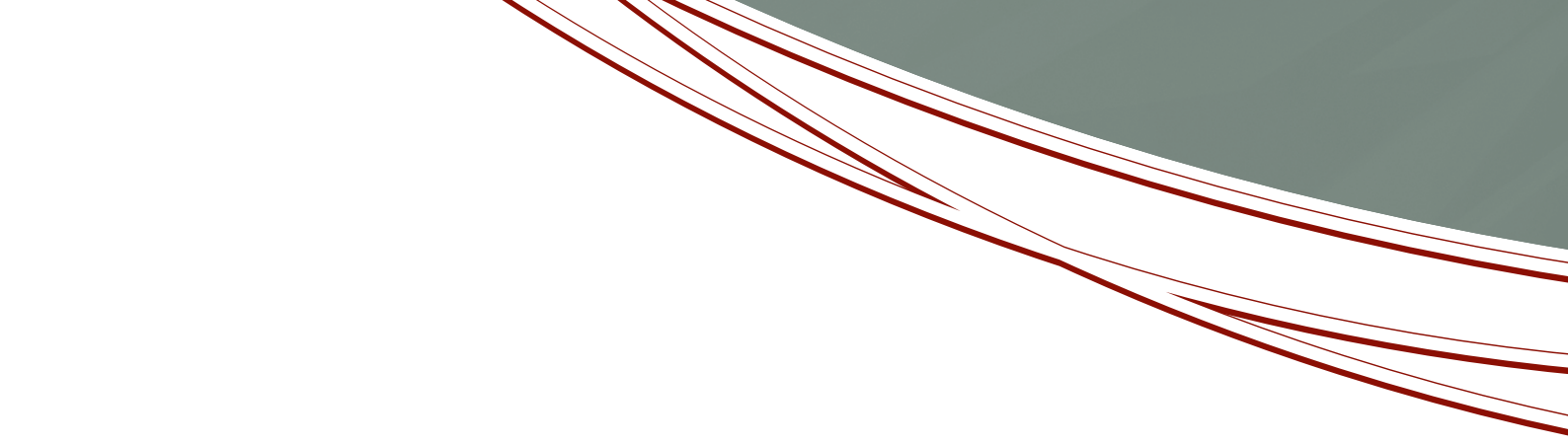
**Table 4: Due diligence conducted for different levels of maturity**

Maturity level	Breadth of screening	Risk basis of screening
Low	<ul style="list-style-type: none"> <li>Limited to employees and very large suppliers.</li> <li>At best, checking only considers<sup>8</sup> basic identity, integrity and credential checks<sup>9</sup>, and often not all of these categories.</li> </ul>	<ul style="list-style-type: none"> <li>Risk is not used as the basis for determining what due diligence to conduct, leading to inconsistency.</li> <li>Rechecking rarely, if ever, occurs.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Includes most staff and suppliers – unlikely to include other organisational associates.</li> <li>Checking usually considers basic identity, integrity and credential checks but may also include a small number of other checks.</li> </ul>	<ul style="list-style-type: none"> <li>Formal requirement to use a risk-basis when conducting due diligence. While some risk categories may be listed, there is little process or guidance to help assess risk and match screening to assessed risk.</li> <li>Rechecking is carried out when substantial additional delegation is added.</li> </ul>
High	<ul style="list-style-type: none"> <li>Mapping of roles is used to determine which staff and organisational associates should be subject to due diligence screening.</li> <li>Checking usually considers a broad range of identity, integrity and credential checks.</li> </ul>	<ul style="list-style-type: none"> <li>Formal assessment conducted of risks associated with employment role, contract, et cetera, with documented and routine processes that ensure that appropriate checks are conducted for assessed risk profile.</li> <li>Rechecking carried out when there is substantial additional delegation and on a regular basis as indicated by analysed risk.</li> </ul>

<sup>7</sup> NSW ICAC, *Strengthening employment screening practices in the NSW public sector*, Sydney, February 2018; NSW ICAC, *Supplier due diligence: a guide for NSW public sector agencies*, Sydney, June 2020.

<sup>8</sup> “Considers” is used here because of the need to screen using a risk basis.

<sup>9</sup> Essentially, identity checks verify that the entity is who they say they are, integrity checks verify that there are no known integrity issues with the entity and credential checks verify the entity has appropriate and/or claimed skills, qualifications and experience.



---

Additional considerations when conducting due diligence are how:

- information supplied to an agency is verified, as opposed to being accepted on face value
- relevant legal and industrial issues are managed.

## Integrity breaches are not tolerated

Despite the best due diligence efforts, agencies will inevitably need to manage situations where individuals have breached integrity standards.

When this occurs, the agency should respond in a manner that is consistent, transparent and proportionate. This is sometimes referred to as a “no misconduct rule”. Similarly, a “no bystander rule” should be used to require individuals to report suspected integrity breaches.

A common rationale for tolerating integrity breaches is that the wrongdoer is valuable to the agency despite their conduct (for example, performance history, seniority, length of tenure, skills profile). For instance, agencies might feel justified in disregarding a case of resume fraud if the employee is a high performer. Indulging in this rationale undermines agency proclamations that it does not tolerate misconduct and can substantially damage efforts to build integrity.

Responding to integrity breaches is the focus of chapter 6, where a detailed discussion of relevant maturity issues can be found.

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to building integrity:

- 3.2 Promoting a sound integrity framework
- 3.3 Managing conflicts of interest
- 3.4 Managing risks connected to gifts, hospitality, donations and similar benefits
- 3.6 Managing performance-based targets
- 3.7 Workforce screening
- 3.8 Screening and ongoing management of business associates

## Chapter 4: Preventing corrupt conduct

Even a highly ethical agency will inevitably work with people who engage in corrupt conduct. Efforts to build integrity can never ensure that everyone is completely ethical all the time – individuals with corrupt intent will sooner or later be able to influence organisational activities. This is not to diminish the role of building integrity but to simply acknowledge that it is only one element of corruption control.

Consequently, agencies need mechanisms to prevent individuals with direct or indirect access to organisational systems and resources from engaging in corrupt conduct. While it would be ideal to have mechanisms in place that literally stop individuals from engaging in corrupt conduct, these sorts of measures are usually only practical for very high-risk systems and processes.

As a result, many prevention measures are aimed at deterring or disincentivising corruption, rather than completely stopping it. This is usually achieved by making the conduct more difficult to carry out, lowering the likely rewards or benefits, or forcing corrupt individuals to take more risks.

Corruption prevention measures can be placed in five broad categories:

- enhancing organisational performance
- developing an agency's integrity policy framework
- identifying corruption vulnerabilities
- protecting specific systems and processes
- enhancing the design of work arrangements.

### Enhancing organisational performance

It is an unfortunate myth that mechanisms aimed at controlling corruption impede organisational performance. In the Commission's experience, the opposite claim is true, and its investigation reports are replete with examples where poor management of organisational performance has facilitated corrupt conduct.

It is much harder to engage in corrupt conduct in a workplace that carefully plans its activities, operates in an efficient and effective manner, obtains value for money and minimises waste. Therefore, the Commission encourages agencies to regard good organisational performance and corruption prevention as complementary activities.

The key outcome is that organisational performance is robustly managed.

While this outcome is critical for corruption control, it relates more to general organisational management than corruption control. Consequently, maturity tables have not been prepared for it.

### Developing the integrity policy framework

For obvious reasons, agencies must have a suite of integrity-related policies.

Key outcomes of this policy framework are that:

- its coverage of integrity issues is sufficient to clearly articulate relevant requirements
- integrity policies are communicated in a manner that ensures these requirements are understood
- the agency ensures compliance with these requirements.

Table 5 presents how elements of an agency's integrity policy framework are typically implemented for cases of

Low, Medium and High corruption control maturity.

**Table 5: Features of integrity policy framework**

Maturity	Coverage	Communication	Enforcement
<b>Low</b>	<ul style="list-style-type: none"> <li>Integrity is addressed in the code of conduct.</li> <li>Generic or principles-based policy requirements exist.</li> </ul>	<ul style="list-style-type: none"> <li>Communication of policy documents is inconsistent, and there may be no communication regarding new or updated policies.</li> </ul>	<ul style="list-style-type: none"> <li>Heavy focus on self-compliance.</li> <li>Otherwise, enforcement occurs following a formal complaint.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Suite of integrity policies exists that addresses topics including (at a minimum) conflicts of interest, gifts and benefits, information security, use of public funds and internal reporting.</li> <li>Specific policy requirements are included.</li> </ul>	<ul style="list-style-type: none"> <li>A standard process is followed to announce and circulate new and updated policy documents.</li> </ul>	<ul style="list-style-type: none"> <li>Managers are responsible for ensuring compliance.</li> <li>Senior management is accountable for serious or systemic policy breaches.</li> <li>Selected Line 3 assurance activity is conducted.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Supporting documentation is in place, such as workflows, procedures, FAQs and templates, which clarifies and provides further detail regarding requirements.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Key points from policy documents, including relevant subject matter experts, are communicated when they are circulated.</li> <li>Resources (for example, tip sheets, training modules) are often developed, and training is provided.<sup>10</sup></li> </ul>	<ul style="list-style-type: none"> <li>As per Medium</li> <li>Line 2 subject matter experts are responsible for developing and implementing compliance controls.</li> <li>Associated workflows and databases align with policy requirements and promote compliance with little effort.</li> <li>There is reporting to the ARC and other governance bodies on compliance activities, compliance breaches, root cause of compliance breaches and how compliance breaches affect organisational risks.</li> </ul>

<sup>10</sup> Integrity training is also discussed in chapter 3.



## Identifying corruption vulnerabilities

While good organisational performance management and integrity policies will help manage corruption risks in general, there are often specific functions, activities, or even roles or business units that carry additional corruption risks. Identifying corruption vulnerabilities is thus an important part of better practice corruption control.

Key outcomes are that:

- frontline managers use their understanding of corruption risk to identify vulnerabilities

- specialist corruption control units continually update and share their understanding of corruption vulnerabilities
- an independent internal audit unit identifies corruption vulnerabilities as part of its work.

Table 6 presents how each line of defence helps identify corruption vulnerabilities for typical cases of Low, Medium and High corruption control maturity.

**Table 6: Identifying corruption vulnerabilities**

Maturity	Frontline managers	Corruption control specialist	Internal audit
<b>Low</b>	<ul style="list-style-type: none"> <li>• Can identify obvious vulnerabilities within their remit.</li> </ul>	<ul style="list-style-type: none"> <li>• Consults other line 2 experts (for example, enterprise risk, governance units).</li> <li>• Monitors reports produced by specialist organisations.<sup>11</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Comments on specific corruption vulnerabilities are observed in audits.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Detailed knowledge of corruption risks and controls applicable to their remit allows for most vulnerabilities within that remit to be identified.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Consults owners of vulnerable systems and processes.</li> <li>• Reviews agency misconduct and near-miss reports.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Potential corruption vulnerabilities are explicitly considered when planning audits and audit programs</li> <li>• Comments are made on any observed patterns of corruption control weaknesses.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Can identify corruption vulnerabilities related to activities outside their remit.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Conducts program of obtaining input and advice from specialist organisations and other corruption control experts.<sup>12</sup></li> <li>• Consults individuals conducting assurance activities regarding vulnerable systems or processes.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Conducts corruption control focused audits.</li> <li>• Corrupt conduct is explicitly or implicitly included in the scope of audits.</li> <li>• Provides assurance over corruption control functions.</li> </ul>

<sup>11</sup> This could be, for instance, an agency such as the Commission or a consultancy firm that has expertise in an area associated with corruption control.

<sup>12</sup> For instance, peers in other agencies.

It should also be noted that the knowledge held by corruption control specialists is of little benefit if it is not used by the agency.

Table 7 presents how corruption control specialist knowledge is distributed to other parts of the agency for cases of Low, Medium and High maturity.

## Protecting vulnerable systems and processes

An agency often has widely-used systems and processes that are particularly vulnerable to corrupt conduct. One example common to all agencies would be their ICT systems. Given these systems are both vulnerable and frequently used, failing to protect them can markedly increase an agency's exposure to corruption risk.

Key outcomes are that:

- more stringent controls are applied to high-risk processes and systems
- the residual level of corruption risk is monitored
- timely and appropriate action is taken in response to audit and review findings.

## Use of more stringent controls

If risk is used as the basis for decision-making, it logically follows that a more stringent suite of controls should be used to protect high-risk systems and processes.

Given the maturity of corruption risk management is the focus of chapter 7, maturity tables are not necessary for this section.

## Managing the residual level of corruption risk

While an agency may implement a suite of general corruption controls, high risk areas may still require additional attention. Consequently, better practice corruption control attempts to manage residual corruption risk and gain assurance that its vulnerable systems and processes are protected.

The type of management required will naturally vary according to the nature of the corruption risks in question. There are, however, some approaches that can be applied. These include the management of:

- potential integrity violations (which is discussed in chapter 6)
- declarations registers (for example, conflicts of interest, or gifts and benefits)
- information holdings
- high-risk transactions and projects.

Table 8, on page 23, presents how this monitoring is typically performed in cases of Low, Medium and High maturity.

**Table 7: Distribution of corruption control specialist knowledge of corruption vulnerabilities**

Maturity	Information to frontline managers	Embedding consideration of corruption risk
Low	<ul style="list-style-type: none"> <li>Information about corruption vulnerabilities is provided on request.</li> </ul>	<ul style="list-style-type: none"> <li>Little involvement in the development or review of organisational systems and processes.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>As per Low</li> <li>Routine provision of information about corruption vulnerabilities but not tailored to specific Line 1 functions.</li> </ul>	<ul style="list-style-type: none"> <li>Usually provides input on potential corruption vulnerabilities that apply to new or revised systems and processes.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium, but efforts are made to tailor information to specific Line 1 managers.</li> <li>Planned program identifies and addresses gaps in understanding of corruption vulnerabilities.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Further input is usually provided to assist implementation.</li> </ul>

**Table 8: Monitoring of declarations registers, information holdings, and high-risk transactions and projects**

Maturity	Declarations registers	Information holdings	Transactions and projects
<b>Low</b>	<ul style="list-style-type: none"> <li>Problematic declarations are flagged in ad hoc manner, usually by frontline management.</li> <li>Minimal monitoring is conducted by specialist units.</li> <li>Declarations may not be held centrally.</li> </ul>	<ul style="list-style-type: none"> <li>Requirement exists to classify the sensitivity of information.</li> </ul>	<ul style="list-style-type: none"> <li>Manager determines whether a given project or transaction is high risk.</li> <li>Manager takes steps to ensure the routine risk management process considers corruption and integrity.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Declarations are stored centrally.</li> <li>Specialist unit monitors declarations.</li> <li>Issues with specific declarations are escalated through usual management channels.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Spot checks are made to ensure that information has been classified correctly and that particularly sensitive information has been handled appropriately.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low, but manager is provided with examples of high-risk transactions and projects to guide their judgment.</li> <li>Additional controls, specific to the transaction or project are imposed (for example, training, conflicts of interest requirements, due diligence and information security).</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Trend analysis is periodically conducted and reported to senior management and/or the ARC.</li> <li>Declarations are supported by periodic attestations and reminders.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>A process is adopted to identify and declassify information that is no longer sensitive (or should never have been classified as sensitive).</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium, but whether a project is high risk is determined by a formal assessment against established criteria, which may involve multiple parties.</li> <li>A probity specialist or similar officer (internal or external) is allocated, and this individual has some authority to direct the implementation of controls and escalate issues to senior management or the ARC.</li> </ul>

## Action in response to audits and reviews

Despite the existence of robust performance and policy frameworks, and controls being placed on vulnerable systems and processes, there will be times when organisational requirements are not being met. Indeed, well-implemented performance and policy frameworks should have mechanisms that help identify when they are not being followed. While specific incidents are usually identified via frontline management, patterns of incidents are more often identified by assurance activity such as reviews and audits.

Such reviews and audits can identify important issues regarding the functioning of systems and processes, including weaknesses in documented systems and processes or failures to comply with them. These issues can create corruption vulnerabilities and impair organisational performance.

Table 9 presents how these elements of responding to audits and reviews typically occur in practice for cases of Low, Medium and High corruption control maturity.

## Process and system design

The design of processes and systems can greatly influence the likelihood of corrupt conduct. For instance, corruption vulnerabilities are created in a process if one person has control over all the steps, no one is accountable for process steps or outcomes, and/or it is very difficult to obtain reliable information about how the process occurred in practice.

By contrast, work designed to have segregation of duties (SoDs), clear accountabilities and which results in reliable information being readily available to someone overseeing or reviewing the processes, makes corrupt conduct difficult to achieve.

Key outcomes are that:

- segregations of duties are considered and enforced
- clear accountabilities are set
- reliable information is readily available to someone overseeing or reviewing the process.

**Table 9: Response to audits and reviews**

Maturity	Action taken	Timeliness of action	Responsibilities and accountabilities
<b>Low</b>	<ul style="list-style-type: none"> <li>• Reports are often viewed as a “compliance nuisance” rather than an opportunity to improve systems and processes.</li> </ul>	<ul style="list-style-type: none"> <li>• Agreed actions have timeframes attached to them.</li> </ul>	<ul style="list-style-type: none"> <li>• There are unclear or unassigned responsibilities and accountabilities surrounding implementation.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• Recommendations and observations made in reports are reviewed by management and actioned if deemed suitable.</li> </ul>	<ul style="list-style-type: none"> <li>• The status of implementation of actions is reported to senior management, although this may only be via exception reporting (that is, when timeframes are not met).</li> </ul>	<ul style="list-style-type: none"> <li>• There are clear responsibilities to meet implementation timelines.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Formal analysis is undertaken to ensure that actions taken are commensurate with risk.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium, but this happens regardless of whether timeframes are met.</li> <li>• Implementing actions in a timely fashion is a performance indicator for applicable managers.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium</li> <li>• Implementation failures are linked to performance assessment.</li> </ul>

Table 10 presents how these factors typically influence work design in cases of Low, Medium and High corruption control maturity.

**Table 10: Process and work design**

Maturity	Segregations of duties	Accountabilities	Information
<b>Low</b>	<ul style="list-style-type: none"> <li>Consideration of SoDs is limited to statutory requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Process is designed in accordance with the agency's delegations framework.</li> <li>Managers hold staff to account but in an ad hoc manner.</li> </ul>	<ul style="list-style-type: none"> <li>Requirement to keep records of business value.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>SoDs is considered a routine part of designing systems and processes, and is informed by corruption risk analysis (see chapter 7).</li> <li>Required SoDs is recorded as part of process/system description.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low, but managers have some established routines for holding staff to account in relation to key decisions.</li> <li>Accountabilities are assigned for key process steps and specified use of agency systems.</li> </ul>	<ul style="list-style-type: none"> <li>Specification of which records should be kept as part of the process step or system usage.</li> <li>Requirement to place records in agency's document and recordkeeping system.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>SoDs is enforced by automated controls in relevant ICT systems and workflows.</li> <li>Assurance mechanisms are adopted to ensure that SoDs is being observed.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium, but managers habitually hold staff to account for the way they use public funds and discretion, based on a sound understanding of corruption risk.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Where possible, work design leverages ICT systems to ensure that accessible records are automatically created.</li> </ul>

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to preventing corrupt conduct:

- 3.2 Promoting a sound integrity framework
- 3.5 Internal controls and the internal control environment
- 3.6 Managing performance-based targets
- 3.8 Screening and ongoing management of business associates
- 3.9 Preventing technology-enabled fraud
- 3.10 Physical security and asset management

## Chapter 5: Detecting corrupt conduct

While effective mechanisms to build integrity and prevent corrupt conduct will substantially decrease the amount and severity of such conduct experienced by an agency, it is ultimately impossible to design functional organisational systems that stop all corruption before it happens.

For this reason, agencies need mechanisms to identify corrupt conduct. While these mechanisms primarily aim to reduce the impact of such conduct, they can also reduce its likelihood, as the credible threat of detection can have a deterrent effect.

There are two key types of mechanisms to detect corrupt conduct:

- those relating to complaints about wrongdoing
- those involving review and analysis of organisational activities.

### Complaint mechanisms

Research across both the public and private sectors consistently shows that corrupt conduct is detected most frequently via complaints from knowledgeable insiders, such as staff and organisational associates. Motivating such individuals to report their concerns helps the agency detect corrupt conduct. This can apply even if these individuals suspect wrongdoing other than corrupt conduct. For instance, someone may report an overpriced contract as waste, when in fact the transaction involved payment of a corrupt benefit.

Related research also shows that trust is a key factor in motivating individuals to report wrongdoing. Staff who want to do the “right thing” may still opt not to report wrongdoing if they lack confidence in an agency’s reporting systems.

Key outcomes are that:

- complainants find it easy to make a complaint
- the agency demonstrates that it genuinely values complaints
- complaint handling processes manage relevant risks.

Underlying all three of these outcomes is the existence of an established complaints handling process, which is a key outcome in itself. Without a documented approach to managing complaints, it is nearly impossible for these outcomes to be achieved because:

- it is difficult for individuals to know how to make a complaint
- the agency (perhaps unintentionally) sends a message that it does not want to receive complaints
- measures to control complaint handling risks cannot be systematically implemented.

### Ease of making complaints

The best complaint handling processes are, of course, of limited value if people are unwilling or unable to make complaints. Better practice corruption control includes making it easy for people to make complaints. This increases the number of complaints received and, ultimately, the number of credible reports of wrongdoing.

Providing support and assistance to people who wish to make a complaint is one key element of making the complaints process easier.

A key element affecting the ease of complaint making is who in an agency can receive a complaint. Mature systems allow for many individuals who vary in seniority,

geographical location and business units to receive complaints. Pursuant to the *Public Interest Disclosures Act 2022* (“the PID Act”)<sup>13</sup>, any public official can make a PID to their manager. Consequently, compliance with the PID Act will achieve this outcome, so long as the agency has sufficient additional options for individuals who wish to report outside their managerial chain.

Table 11 presents how other key elements affect the ease of complaint making for typical cases of Low, Medium and High corruption control maturity.

**Table 11: Features affecting ease of complaint making**

Maturity level	Straightforwardness	Multiple modes	Anonymity supported
<b>Low</b>	<ul style="list-style-type: none"> <li>Complaints making process is complex and difficult to understand.</li> </ul>	<ul style="list-style-type: none"> <li>Verbal PIDs are discouraged.<sup>14</sup></li> <li>Other complaints must be made in writing.</li> </ul>	<ul style="list-style-type: none"> <li>Anonymous PIDs are discouraged.<sup>15</sup></li> <li>Other complaints cannot be made anonymously.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Complaints process is clear but inflexible.</li> </ul>	<ul style="list-style-type: none"> <li>Complaints can be made verbally or in writing.</li> </ul>	<ul style="list-style-type: none"> <li>Anonymous complaints are allowed and not discouraged.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>Complaints process is clearly described and can handle situations where it is not followed exactly as planned by a complainant (for example, a complainant breaching confidentiality or withdrawing their cooperation).<sup>16</sup></li> </ul>	<ul style="list-style-type: none"> <li>Complaints can be made by telephone, in person or in writing, and via mechanisms such as hotlines and webforms.</li> </ul>	<ul style="list-style-type: none"> <li>The ability to readily make anonymous complaints is embedded into the design of reporting channels.</li> <li>Provisions exist to support anonymous complainants who later choose to identify themselves.</li> </ul>

<sup>13</sup> While the *Public Interest Disclosures Act 1994* is still in force and the PID Act may not commence until late 2023, this chapter has considered the latter’s provisions.

<sup>14</sup> Under the PID Act, it is illegal to prohibit verbal PIDs.

<sup>15</sup> Under the PID Act, it is illegal to prohibit anonymous PIDs.

<sup>16</sup> The management of misdirected complaints is discussed later in this chapter.



## Reporting is valued by the agency

An agency which demonstrates that it values complaints may encourage reluctant individuals to report alleged wrongdoing.

Taking disciplinary or other action against wrongdoers, and where appropriate communicating that action was taken, is a critical step that an agency can take to demonstrate that it values complaints. This is discussed in more detail in chapter 6.

Protecting reporters, for instance as per the PID Act, can also show that reporting is valued. Broadly speaking, agencies should take all reasonable steps to ensure that anyone making a complaint is not adversely affected as a result. This is discussed in the “Formal complaint processes that manage associated risks” section of this chapter.

Two other key things that an agency can do to show that it values complaints are:

- actively promoting complaint making
- using complaints to inform organisational improvements or assurance initiatives.

Table 12 presents how agencies demonstrate that they value complaints for typical cases of Low, Medium and High corruption control maturity.

## Complaint handling processes that manage associated risks

Three key things that can make a complaint handling process ineffective are that:<sup>17</sup>

- it only considers complaints from select entities (for example, staff can make complaints but organisational associates cannot)
- complaints are not managed appropriately if they are sent through the “wrong channel” (for example, if corrupt conduct allegations are reported to a workplace health and safety hotline) – this publication terms these “misdirected complaints”
- there is insufficient management of the risk of detrimental action or conflict.

For obvious reasons, compliance with the PID Act is also important.

Table 13, on page 29, presents features of complaint handling processes for typical cases of Low, Medium and High corruption control maturity.

**Table 12: Features demonstrating that an agency values complaints**

Maturity level	Promoting complaint making	Informing organisational improvement
<b>Low</b>	<ul style="list-style-type: none"> <li>Complaint making is listed as important in policy documents.</li> </ul>	<ul style="list-style-type: none"> <li>The agency makes no attempt to utilise information from complaints except in the specific context of handling them.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Complaint making is encouraged in mandatory training.</li> </ul>	<ul style="list-style-type: none"> <li>Informal information is passed to affected business units about potential systemic weaknesses identified from complaints.</li> <li>System changes that are ultimately made are not linked to the complaint.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Complaint making is promoted in communications from senior executives.</li> </ul>	<ul style="list-style-type: none"> <li>Information related to affected systems is formally passed back to business units to consider changes.</li> <li>Where appropriate, changes arising from complaints are communicated to staff including complaints identified as PIDs.</li> </ul>

<sup>17</sup> Risks regarding the taking of action following a complaint, such as disciplinary action, are discussed in chapter 6.

**Table 13: Features of complaint handling processes**

Maturity level	Who can complain	Misdirected complaints	Detrimental action and conflict	PID Act compliance
<b>Low</b>	<ul style="list-style-type: none"> <li>Only staff (or possibly only employees and onsite contractors) can make complaints.</li> </ul>	<ul style="list-style-type: none"> <li>No formal processes exist that deal with misdirected complaints.</li> </ul>	<ul style="list-style-type: none"> <li>While a policy statement against reprisals exists, there are no practical mechanisms to manage reprisal risks.</li> </ul>	<ul style="list-style-type: none"> <li>While the internal reporting policy states that complaints are managed in accordance with the PID Act, a formal review of PID Act requirements does not inform the development of complaint handling processes.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>The capacity to take complaints from organisational associates and possibly other external parties exists but is not promoted.</li> </ul>	<ul style="list-style-type: none"> <li>Local processes to handle misdirected complaints exist but there is minimal coordination across different complaint handling units.</li> </ul>	<ul style="list-style-type: none"> <li>There is a requirement to document risks of detrimental action and conflict.</li> </ul>	<ul style="list-style-type: none"> <li>Complaint handling processes are informed by a formal review of PID Act requirements.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>Reporting channels exist for all staff, organisational associates and other external parties, and are systematically promoted to all relevant parties.</li> </ul>	<ul style="list-style-type: none"> <li>There is a coordinated approach across different complaints channels to ensure that complaints are consistently triaged, and misdirected complaints are redirected to the correct channel.</li> </ul>	<ul style="list-style-type: none"> <li>Detrimental action and conflicts are subject to formal risk management, with ongoing monitoring of effectiveness.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Compliance with the PID Act is formally incorporated into the organisation's assurance framework.</li> <li>A formal PID risk management process is adopted and regularly reviewed.</li> </ul>

## Review and analysis mechanisms

While complaints are very important, agencies cannot rely on them as the sole mechanism by which to detect corrupt conduct. For instance, some individuals may not be aware of extant corrupt conduct, especially if it has only recently commenced. Alternatively, they be aware but may choose not to report it.

Because of this, better practice corruption control adopts a range of review and analysis mechanisms to detect corrupt conduct.

Key outcomes are that:

- the frontline routinely checks for red flags of corrupt conduct and organisational systems support the review of these flags
- assurance units use a range of additional measures to identify potential corrupt conduct.

## Checking by the frontline

Frontline staff (that is, Line 1 units<sup>18</sup>) are often in a good position to detect certain types of corrupt conduct. This is because they have a good grasp of what is “normal” within their spheres of operation, including when local controls or processes are being bypassed or compromised.

Table 14 presents frontline checking activities for typical cases of Low, Medium and High corruption control maturity.

Frontline non-managerial staff are also able to assist with checking. Agencies can support staff to do this by informing them of red flags relevant to their work and having systems in place to review any red flags they raise.

## Checking by assurance units

While frontline checking can be useful for spotting unusual activity, better practice corruption control also has dedicated checking processes within assurance units (especially Line 2 units). This is because frontline checking:

- may not always be performed effectively
- is not often designed to pick up unusual patterns of activity, including activity that involves multiple business units or processes.

Table 15, on page 31, presents assurance unit checking for typical cases of Low, Medium and High corruption control maturity.

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to detecting corrupt conduct:

- 4.2 Post-transactional review
- 4.3 Analysis of management accounting reports
- 4.4 Identification of early warning signs
- 4.5 Data analytics
- 4.6 Fraud and corruption reporting channels
- 4.7 Whistleblower management systems
- 4.8 Leveraging relationships with business associates and other external parties
- 4.9 Complaint management
- 4.10 Exit interviews

**Table 14: Features of frontline checking for different levels of maturity**

Maturity	Frontline managers	Corporate units
Low	<ul style="list-style-type: none"> <li>Expected to act if they come across a red flag but they do not conduct planned monitoring or checking activities to find red flags.</li> </ul>	<ul style="list-style-type: none"> <li>Perform business-as-usual checks on transactions but without any conscious regard to integrity-related red flags.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Monitor activities for red flags within their purview.</li> <li>Monitor their budget and cost centre(s).</li> </ul>	<ul style="list-style-type: none"> <li>Some integrity-related checks are performed on transactions but these are not coordinated with documented risks.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Are aware of relevant corruption risks and associated red flags, and use this information to guide their monitoring activities.</li> <li>Follow-up red flags referred to them (for example, by their subordinates).</li> <li>Run specified integrity checks regarding their finances and staffing arrangements.</li> </ul>	<ul style="list-style-type: none"> <li>Planned program of specific integrity-related checks to be conducted that is coordinated with documented risk.</li> <li>Organisational systems encourage and support pursuing issues with other business units.</li> </ul>

<sup>18</sup> As per the three lines of defence model defined in chapter 1.

**Table 15: Features of assurance unit checking**

Maturity level	Obtaining expert input	Probity monitoring	Data analytics program	Use of external audit
<b>Low</b>	<ul style="list-style-type: none"> <li>No consultation with process experts or corruption control experts is conducted when designing checking programs.</li> </ul>	<ul style="list-style-type: none"> <li>Available to respond to probity queries, such as reviewing declarations.</li> </ul>	<ul style="list-style-type: none"> <li>No formal program.</li> <li>No processes exist to communicate insights to other parts of the agency.</li> </ul>	<ul style="list-style-type: none"> <li>Limited use of external audit for detection purposes.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Process experts and corruption control experts are consulted about scope and design.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Proactively examines probity-related data, perhaps using random sampling, to identify suspicious activity.</li> </ul>	<ul style="list-style-type: none"> <li>Program is limited to key datasets<sup>19</sup> with limited capacity to merge datasets.</li> <li>Informal processes exist to communicate insights to the agency.</li> </ul>	<ul style="list-style-type: none"> <li>Agency genuinely considers management letters as a source that can be used to help identify potential corrupt conduct.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Process experts and corruption control experts are consulted about assurance activities.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Data analytics program is leveraged to conduct targeted sampling of probity-related data.</li> </ul>	<ul style="list-style-type: none"> <li>Program examines data from a range of organisational datasets with capacity to readily merge different datasets.</li> <li>Both formal reporting on the program and informal communication of insights occur.</li> <li>Process is in place for escalating red flags for further examination.</li> </ul>	<ul style="list-style-type: none"> <li>Auditors are encouraged to look for activity that might suggest potential corrupt conduct and flag it, and their input is considered and actioned where appropriate.</li> </ul>

<sup>19</sup> This varies from agency to agency. Sometimes this is datasets such as accounts payable and procurement data. Other times this is agency specific datasets, such as register of enforcement of specific regulatory requirements.

## Chapter 6: Responding to integrity breaches

What action an agency takes when integrity breaches are detected is critical to its corruption control efforts. While agencies should address breaches in an objective and impartial way, if the response to an established breach is perceived as insufficient it sends a tacit message that the agency either tolerates such conduct or otherwise views it as unimportant. This can undermine its corruption control efforts in two ways.

First, it can increase the risk of further corrupt conduct. For integrity breaches that constitute corrupt conduct, an insufficient response may encourage the wrongdoer or other individuals to engage in similar acts in the future. For breaches that do not constitute corrupt conduct, an insufficient response can lead to an escalation of unethical behaviour that ultimately results in corrupt conduct.

Secondly, perceptions that integrity breaches are not viewed as important undermine other corruption control elements. In particular, such perceptions both make attempts to promote integrity and prevent corruption (see chapters 3 and 4 respectively) appear hollow, and deter reporting of suspected wrongdoing (see chapter 5).

There are three key elements to the way an agency responds to integrity breaches:

- timely and proportionate action is taken in response to specific breaches
- patterns of breaches are analysed
- insights from integrity breaches inform an agency's corruption control program.

### Responding to specific breaches

To ensure that the message that “something will be done” is heard, it is important to respond to each integrity breach in a proportionate manner. This should apply regardless of factors such as an individual's role, seniority or employment status – there should not be any “protected species”.

Two key outcomes are:

- alleged integrity breaches constituting corrupt conduct or other serious misconduct are appropriately reported externally by agencies and investigated
- proportionate action is taken in response to established integrity breaches.

### Alleged corrupt conduct or other serious misconduct

Alleged integrity breaches that constitute corrupt conduct usually require additional scrutiny. In addition to such allegations constituting more substantial ethical violations, they are also likely to trigger legal or regulatory obligations.

For instance, if the head of an agency has a reasonable suspicion of corrupt conduct, it must be reported to the Commission under s 11 of the ICAC Act. Additional reporting to organisations such as the NSW Police Force, NSW Ombudsman, Audit Office of NSW or other regulatory agencies may be required.

Agencies may also internally investigate alleged corrupt conduct. For instance, the Commission might choose not to investigate a matter, but the agency wishes to know whether the allegations can be substantiated and to take relevant action if it is.

Table 16 presents how agencies respond to alleged corrupt conduct for typical cases of Low, Medium and High corruption control maturity.

It is also not unusual for evidence of corrupt conduct to emerge during an investigation into a different type of conduct. A capable investigations function can adapt to such unexpected changes in direction, but a low-level maturity unit often fails to respond to evidence of more serious misconduct.

## Considering a range of action

As integrity breaches vary in terms of seriousness, a one-size-fits-all response is not useful. For instance, an approach focused on training and counselling could allow serious misconduct to go unpunished, but undertaking a comprehensive investigation into every allegation could preclude opportunities to address minor misconduct in a timely and effective manner.

**Table 16: Response to alleged corrupt conduct**

Maturity	External reporting	Internal investigation
<b>Low</b>	<ul style="list-style-type: none"> <li>While a willingness to report may exist, there is an ad hoc approach with no clear internal process.</li> </ul>	<ul style="list-style-type: none"> <li>Investigations unit or officer is tasked with investigating alleged corrupt conduct.<sup>20</sup></li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Systematic, documented approach exists for reporting misconduct-related matters to external parties, including the Commission.</li> <li>Compliance with PID Act reporting obligations.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Investigators have the skills, experience and knowledge (including a good working knowledge of the PID Act), and resourcing and powers to rigorously investigate most types of alleged corrupt conduct.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium</li> <li>Agency actively cooperates with external agencies to resolve misconduct incidents, even when under no obligation to do so.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Investigators have the skills, experience and knowledge, and resourcing and powers to rigorously conduct even complex or challenging investigations (for example, collusion involving multiple public officials, covert investigations into senior management).</li> </ul>

<sup>20</sup> Note that an investigations unit may be inhouse or predominantly outsourced. In practice, an agency's investigative unit(s) will investigate a range of misconduct types in addition to corrupt conduct.

Moreover, a one-size-fits-all approach may fail to adequately address any control issues. For instance, if an undeclared conflict of interest regarding a supplier was detected as part of a routine due diligence program, that would likely indicate the program was operating effectively (although it might also indicate a lack of compliance with disclosure requirements). By contrast, if the conflict of interest was only detected after the supplier had committed a large fraud against the agency, it would likely represent a control weakness. A one-size-fits-all approach lacks the nuance to deal with these different circumstances.

Consequently, better practice corruption control involves considering a range of possible actions in response to a specific integrity breach and adopting those that are most appropriate (for example, proportionate to the severity of the breach and the agreed risk).

Three key types of actions to consider in response to an integrity breach are actions taken:

- against the wrongdoer
- to remediate control weaknesses
- to inform staff, both managerial and non-managerial, that an integrity breach has been detected.

In relation to the third point, things like privacy considerations can present challenges. However, there is a variety of options an agency can use including deidentified or summarised reporting and discussing relevant, publicly known examples from other organisations.

In some circumstances, an integrity breach can adversely affect the productivity, morale and wellbeing of staff. On a case-by-case basis, agencies may need to adopt a plan for addressing these issues. While the details of such an approach go beyond the scope of this publication, further guidance can be found in disciplines such as human resources management, change management and crisis management.

Table 17, on page 35, presents what actions from each of these three types are considered (and adopted if appropriate) for typical cases of Low, Medium and High corruption control maturity.



**Table 17: Response to integrity breaches**

Maturity	Against wrongdoer	Remedying control weaknesses	Informing staff
<b>Low</b>	<ul style="list-style-type: none"> <li>Strong disciplinary action is taken in response to severe breaches. Most other action is informal and ad hoc.</li> <li>There is little meaningful response if the wrongdoer is not a staff member.</li> </ul>	<ul style="list-style-type: none"> <li>There is little reflection on whether an integrity breach indicates a control weakness.</li> </ul>	<ul style="list-style-type: none"> <li>Little attempt is made to inform staff that the agency has detected integrity breaches.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Range of disciplinary actions (for example, from counselling to dismissal) is considered and adopted if appropriate.</li> <li>Formal process exists for determining which action to adopt.</li> <li>Where possible, will avoid future relationships with organisational associates who commit integrity breaches.</li> </ul>	<ul style="list-style-type: none"> <li>Informal consideration of potential control weaknesses linked to breach.</li> <li>For severe breaches, a formal review of the relevant system might be commissioned.</li> </ul>	<ul style="list-style-type: none"> <li>Workers are told in general terms that the agency has detected integrity breaches and the types of actions it might take in response.</li> <li>Specific examples of detected breaches are provided in exceptional circumstances.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Will take legal and other action (for example, ceasing relationships, complaints to relevant bodies) against organisational associates who commit integrity breaches.</li> <li>Willing to take actions to recover stolen property and funds.</li> </ul>	<ul style="list-style-type: none"> <li>Corruption control specialists and other subject matter experts triage the likely relevance of control weaknesses to the integrity breach and what potential action should be taken in response.</li> <li>Potential action can include informal guidance to managers or other staff, recommendations for changes to systems or processes, or commissioning reviews to further explore the issue.</li> </ul>	<ul style="list-style-type: none"> <li>Where possible, relevant information about integrity breaches, how they were detected and what action was taken in response is communicated to staff.</li> <li>Specific examples of detected breaches are provided where appropriate<sup>21</sup>, including when raised through internal reporting systems.</li> </ul>

<sup>21</sup> As noted earlier, this may not always be possible because of confidentiality requirements. However, the high-level maturity organisation aims to distribute such information where it can, subject to the constraints of these requirements.

## Patterns of breaches

While valuable information about corruption control may be obtained from specific integrity breaches, further insights can often be obtained by analysing patterns of breaches. For instance, a one-off integrity breach may reflect local conditions within a given business unit, but a pattern of similar breaches in multiple business units may reflect a broader organisational control issue.

Additionally, while chapter 5 discusses making systems changes in response to specific complaints of wrongdoing, there are occasions where such changes are difficult to justify; for example, one specific integrity breach may not justify the cost involved in enhancing relevant controls.

An element of better practice corruption control is the review of integrity breaches reports by specialist business units, including the use of trend analysis. Sometimes, such trend analysis can reveal a pattern of integrity breaches that can justify more intensive controls than could be justified from reviewing the individual breaches in isolation. For instance, such a pattern might:

- indicate greater corruption vulnerability, providing a risk-basis for adopting more intensive controls
- provide more information about the nature of control failure or vulnerabilities, facilitating a more tailored enhancement of controls.

The key outcome is that the agency systematically analyses integrity breaches.

Table 18 presents how public authorities analyse integrity breaches for typical cases of Low, Medium and High corruption control maturity.

## Informing corruption control efforts

Reviewing individual integrity breaches and analysing patterns can enhance an agency's understanding of its vulnerabilities. However, this increased understanding is of limited value if it ultimately does not result in more effective corruption control activity.

The key outcome is that insights from integrity breaches are used to enhance an agency's corruption control program.

One key way in which insights from integrity breaches can inform corruption control efforts is to use them to revise systems and processes, including those relating to performance management and accountability. The "Control weaknesses" column in table 17 can also be used to assess maturity for this purpose.

Table 19, on page 37, presents two other ways agencies use insights from integrity breaches to inform corruption control efforts for typical cases of Low, Medium and High corruption control maturity.

**Table 18: How integrity breaches are analysed**

Maturity	Analysis approach
Low	<ul style="list-style-type: none"> <li>• Analysis of integrity breaches considers basic information such as the number of matters identified or investigated.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Analysis of breaches includes variables providing detail about the incident, such as business unit, geographical location, nature of the breach and the function applicable to the breach.</li> </ul>
High	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• There is a dedicated program of analysing integrity breaches that aims to identify the clustering of events, emerging issues and other unusual breaches.</li> </ul>

**Table 19: Use of insights from integrity breaches**

Maturity	Communicating to managers	Incorporating into corruption control plan
<b>Low</b>	<ul style="list-style-type: none"> <li>Generally, only the management of the affected unit(s) is informed. Otherwise, communication is ad hoc or on request.</li> </ul>	<ul style="list-style-type: none"> <li>List of functions that carry additional corruption risk is updated.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Corruption control specialists proactively distribute insights from analyses of integrity breaches to managers across the agency.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Existing risk ratings and descriptions are updated.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>In depth discussions are held with managers to whom insights are particularly relevant.<sup>22</sup></li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>New activities to prevent re-occurrence of the breach and address revised risks are promptly documented in the plan and implemented. This potentially extends beyond the unit(s) affected by the integrity breach.</li> </ul>

## Relevant Australian Standard sections

The following Australian Standard sections are relevant for responding to integrity breaches:

- 5.2 Immediate actions in response to discovery of fraud or corruption
- 5.3 Investigation of a detected fraud or corruption event
- 5.4 Disciplinary procedures
- 5.5 Crisis management following discovery of a fraud or corruption event
- 5.6 Internal reporting and escalation
- 5.7 External reporting
- 5.8 Recovery of stolen funds or property
- 5.9 Responding to fraud and corruption events involving business associates
- 5.10 Insuring against fraud events
- 5.11 Assessing internal controls, systems and processes post-detection of a fraud or corruption event
- 5.12 Third parties
- 5.1.3 Disruption of fraud and corruption

<sup>22</sup> For instance, if there were a pattern across the organisation of not declaring secondary employment, corruption control specialists might further engage with HR managers on this topic.

## Chapter 7: Corruption risk management

The formal management of corruption risk is a critical part of corruption control. To an extent, corruption risk management (CRM) represents a move from the abstract to the concrete. Consistent with the standard on risk management (AS ISO 31000:2018), it involves three key sets of actions:

- the identification and analysis of actual corruption risks (corruption risk assessment), noting that the corruption risk profile of an agency may shift significantly over time (for example, as its role evolves, it merges with other bodies or its means of delivery change)
- the selection and implementation of key preventative<sup>23</sup>, detective and response controls relating to those risks (corruption control adoption)
- measures to provide ongoing assurance, involving each of the three lines (explained in chapter 1), that controls are effective and operating as intended (corruption control assurance).

Agencies must take actions regarding each of these sets. These actions should be at a level and in a form that is appropriate to their nature, needs and circumstances. If this process is compromised, some corruption risks are likely to be under-controlled while others may be over-controlled.

Better practice CRM has the following key features:

- It is integrated with agency business.
- The analysis of corruption risks is performed robustly.
- Controls are selected to effectively and efficiently control corruption risks, and the

agency is mindful of the importance of using different types of controls.

- There are assurance arrangements that monitor the effective operation of both hard and soft corruption controls. This relates to organisational assurance more than corruption control per se and hence discussion of this feature is beyond the scope of this publication.

It should be noted that some elements of better practice CRM correspond to maturity in risk management more generally. Maturity tables have not been provided in such cases but AS ISO 31000:2018 is suggested as an initial point of reference.

### Integration with agency business

One perennial shortcoming with CRM (and with risk management generally) is that it can become divorced from an agency's operations. For instance, corruption risks may be identified and analysed, and controls developed, but this process does not bear upon how processes occur in practice.

This issue can manifest in several different ways. It might be that corruption risks are analysed at an enterprise level but CRM does not occur for programs or projects. Alternatively, CRM may occur during a program's operation but not during its development, or vice versa. CRM might also be viewed merely as a "box ticking" compliance exercise, or a problem to be managed by "head office".

Like all aspects of risk management, CRM requires a holistic approach, using all three lines to provide assurance that corruption risks are being managed appropriately.

<sup>23</sup> Note that this includes the pillars of both building integrity and preventing corrupt conduct.

That is:

- operational management (Line 1) plays a key role in identifying risks, implementing hard controls and building the accompanying soft control environment
- second line specialists support and assist the first line in this endeavour, especially with knowledge building, providing processes and tools, and developing first-line assurance mechanisms
- in practice, corruption control within the agency will often be a Line 2 function; in any case, it is the Commission's view that it should not be a mere adviser to the business – the function should itself be responsible for some but not all corruption controls (although the frontline, other Line 2 units and internal audit (Line 3) should also each be responsible for some corruption controls)
- third line units obtain assurance that CRM arrangements are effective and operating as intended.

Key outcomes are that:

- managing corruption risk is treated as a routine part of an agency's operations
- CRM occurs at strategic, operational and project levels (and, as such, it occurs at levels ranging from enterprise to frontline); this relates to general risk management maturity, so maturity levels have not been provided
- CRM occurs during both planning and development, and operations phases (with the latter including reviews of, and changes to, processes and systems); this is also related to general risk management maturity, so maturity levels have not been provided

- the ownership of corruption risks and controls is located across the agency with corruption control specialists playing a coordinating role.

Table 20, on page 40, presents how CRM integrates with agency activities for typical cases of Low, Medium and High corruption control maturity.

## Robustness of corruption risk analysis

While CRM should be integrated with other agency risk management processes, there are several important differences between corruption risks and other risks.

First, corrupt individuals actively try to defeat existing controls. Compared with most other classes of risk, this is unusual. For instance, while a serious workplace accident might involve some careless behaviour, it would be highly irregular for staff to intend for the accident to occur. Conversely, by definition, corrupt conduct is deliberate and often involves a degree of planning.

Secondly, it can be difficult to test whether a control is effective because corrupt individuals usually try to conceal their conduct. An agency may be unaware for years that existing corruption controls are ineffective. Indeed, an apparent absence of corrupt conduct could be due to:

- the success of corruption controls
- no one attempting to act corruptly
- a failure to detect corrupt conduct that has occurred.

Thirdly, in some environments, individuals engaging in corrupt conduct may collude with others inside and/or outside the agency to facilitate corrupt actions and circumvent controls.

Fourthly, the nature and volume of complaints is not a reliable proxy for actual corrupt conduct. For the reasons stated above, corrupt conduct tends to be under-reported. In addition, some of the complaints an agency does receive alleging corruption will be exaggerated, based on a misinterpretation of legitimate behaviour, or even vexatious.

Fifthly, it is difficult to evaluate the losses or damage that will be caused by a corrupt individual. Some corrupt schemes cause direct financial losses (for example, frauds) but others have a greater effect on decision-making and reputation (for example, bribery). In addition, it is difficult to predict whether certain corruption schemes will be petty or grand in nature, or whether they will be carried out by a junior or senior official, both of which can dramatically affect the size of corrupt losses. For example, a senior executive engaged in an invoicing fraud, and colluding with outside parties, might misappropriate millions of dollars. But invoicing fraud committed by a junior officer acting alone might only misappropriate a fraction of that amount.

Based on these characteristics, determining the likelihood and consequences of many corruption risks involves a degree of guesswork.

While not limited to corrupt conduct, it can also be challenging to assign risk and control owners to corruption risks because multiple business processes may be compromised in a corrupt scheme. While owners of different processes can be each given some responsibility, there is still a need to assign an overall risk owner.

These issues reinforce the need for CRM to include a robust analysis of corruption risk. For instance, documented controls such as “adherence to policy” may do little against an individual determined to act corruptly, especially if part of their corrupt scheme involves not following the policy in question. Moreover, making users of the policy the owners of such a control also seems pointless for the same reason. A robust corruption risk analysis must consider such issues to understand control challenges.

**Table 20: Integration of CRM with agency activities**

Maturity	Routine part of doing business	Ownership of corruption risks and controls
<b>Low</b>	<ul style="list-style-type: none"> <li>CRM is treated as a compliance obligation that is irrelevant to core business.</li> <li>CRM is done “to the agency”.</li> </ul>	<ul style="list-style-type: none"> <li>Risk ownership is concentrated in the agency’s corruption control function.</li> <li>Corruption controls are primarily imposed by this function.</li> <li>CRM essentially functions as a silo.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>CRM is treated as a means of protecting the agency from reputational damage and financial losses.</li> <li>CRM is done “to protect the agency”.</li> </ul>	<ul style="list-style-type: none"> <li>Risk ownership is shared between corruption control and high-risk functions (for example, procurement, accounts payable, payroll, ICT security).</li> <li>Corruption controls are imposed by these functions.</li> <li>CRM essentially functions as a collective of specialist units working together, led by the corruption control function.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>CRM contributes to the effective and efficient achievement of the agency’s outcomes.</li> <li>CRM is part of, or coordinated with, other risk management activities.</li> <li>CRM is done “with the agency”.</li> </ul>	<ul style="list-style-type: none"> <li>Any frontline manager or project manager can “own” a corruption risk or control.</li> <li>The corruption control function has responsibility for coordinating, documenting and reporting overall status of CRM efforts (as discussed in chapters 8 and 9).</li> <li>CRM essentially functions as a hub and spokes model.</li> </ul>

Key outcomes are that:

- corruption risks are analysed using appropriate methodology, standards and approaches; this relates to general risk management maturity, so maturity levels have not been provided
- an agency's operating environment informs its analysis of corruption risks; this also relates to general risk management maturity, so maturity levels have not been provided
- corruption risk analysis is performed with sufficient frequency across the organisation to ensure that an agency's knowledge of its corruption risk profile is current
- when analysing corruption risks, it is explicitly considered that corruption risks may manifest differently across the agency.

Table 21 presents the robustness of corruption risk analysis for typical cases of Low, Medium and High corruption control maturity.

## Effective and efficient corruption controls

As with any risk management process, even the best corruption risk analysis is of little value if it does not guide the adoption of controls. Corruption control is not aided by a detailed analysis, demonstrating that corruption risks are poorly controlled, if that analysis is not used to enhance their control. While a key component of ensuring that corruption controls are effective and efficient is assurance over corruption control activity (as discussed in the "Integration with agency business" section earlier in this chapter), the process used to select controls is also critical.

Key outcomes are that:

- a sufficiently broad range of controls is used<sup>24</sup>
- the application and evaluation of controls supports agency outcomes.

**Table 21: Corruption risk analysis**

Maturity	Frequency	Different manifestation
<b>Low</b>	<ul style="list-style-type: none"> <li>• Single agency-wide corruption risk assessment is conducted approximately every two years.</li> </ul>	<ul style="list-style-type: none"> <li>• Corruption risk analysis considers that corruption risks might manifest differently in different activities.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Corruption risk assessment is sometimes updated in response to specific integrity breaches or patterns of breaches.</li> <li>• Localised corruption risk assessments are conducted when planning new projects and designing/re-designing functions.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Analysis considers that corruption risks might manifest differently in different business units, functions, systems and processes.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• Corruption risks are routinely assessed at any time throughout the agency.</li> <li>• Managers of discrete agency units, programs, projects, contracts et cetera consider assessing corruption risks as part of routine risk management activity.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Risks associated with organisational associates are analysed.</li> <li>• The impact of organisational structure on corruption risk is analysed.</li> </ul>

<sup>24</sup> This does not mean that a broad range of controls is needed for each corruption risk, merely that the organisation displays genuine intellectual openness when considering which controls to select.



## Breadth of controls

Serious corrupt conduct is often associated with an inadequate selection of controls. For instance, an agency may have a reasonable suite of documented policies but few controls in place to ensure compliance.

Three important elements of control breadth are the extent to which:

- controls from each of the four pillars are considered<sup>25</sup>

- different types of controls (for example, soft and hard controls) are considered
- controls are placed on organisational associates.

Table 22 presents the breadth of controls used for typical cases of Low, Medium and High corruption control maturity.

**Table 22: Breadth of controls**

Maturity	Pillars	Types	Organisational associates
Low	<ul style="list-style-type: none"> <li>• Use of each pillar is ad hoc. Whether the applicability of a particular pillar is considered varies from risk to risk.</li> </ul>	<ul style="list-style-type: none"> <li>• Hard controls, most frequently policies and procedures, are used.</li> <li>• Automated controls are rarely adopted.</li> </ul>	<ul style="list-style-type: none"> <li>• There are contractual requirements (for example, to report alleged corrupt conduct by their staff, or to abide by specified ethical standards).</li> </ul>
Medium	<ul style="list-style-type: none"> <li>• There is general consideration of the applicability of each pillar when selecting controls.</li> </ul>	<ul style="list-style-type: none"> <li>• A broad range of hard and soft controls is used.</li> <li>• Key processes may have automated controls.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low</li> <li>• There is communication of ethical standards (for example, briefings, statements of business ethics).</li> <li>• There are requirements to disclose information about certain anti-corruption controls, such as policies, procedures and roles.</li> </ul>
High	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• For high severity risks, controls from all four pillars are used.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium but a planned mix of automated and manual controls is used.</li> <li>• Where applicable, behavioural principles are used to help design or implement controls.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Agency verifies that organisational associates have a suite of proportionate anti-corruption controls. This aims to ensure that there is no net increase in residual corruption risk from dealing with the associate.</li> </ul>

<sup>25</sup> As discussed in chapters 3–6, these pillars are building integrity, preventing corrupt conduct, detecting corrupt conduct, and responding to integrity violations. It should be noted that these four types together include both preventative and detective controls.

## Application of controls

As with any type of risk, corruption risk represents a threat to agency outcomes. The negative effects include, but are not limited to, financial loss, operational underperformance, reputational damage and poor staff morale.

The adoption of corruption controls is thus not simply an end but also a means of helping the agency achieve its outcomes. Adoption of appropriate corruption controls assists the agency to achieve good financial and operational performance, and protect its internal and external reputation.

Two ways in which better practice corruption control acknowledges the importance of agency outcomes are: adopting corruption controls on a basis commensurate with risk; and documenting and evaluating corruption controls to help ensure that they are achieving their desired outcomes. These relate to general risk management maturity, so maturity levels have not been provided.

Table 23 presents additional ways in which corruption controls are applied for typical cases of Low, Medium and High corruption control maturity.

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to corruption risk management:

- 2.4 Specialist fraud and corruption control resourcing
- 2.5 Line management
- 2.6 Business unit accountability for fraud and corruption control
- 2.7 Awareness raising of fraud and corruption risks
- 2.8 Fraud and corruption risk management
- 3.5 Internal controls and the internal control environment

**Table 23: Application of controls**

Maturity	Facilitating outcomes	Coordinating across lines of defence
Low	<ul style="list-style-type: none"><li>Desired agency outcomes are not considered when selecting controls.</li></ul>	<ul style="list-style-type: none"><li>Corruption risk treatments confined to Line 2 or head office.</li></ul>
Medium	<ul style="list-style-type: none"><li>Desired agency outcomes are considered when selecting controls but are usually limited to specific domains (for example, financial performance).</li></ul>	<ul style="list-style-type: none"><li>Some coordination between Lines 2 and 3 (for example, internal audit takes steps to test documented corruption controls).</li><li>Some coordination between Lines 1 and 2 (for example, corruption control specialist liaises with frontline managers).</li></ul>
High	<ul style="list-style-type: none"><li>Desired agency outcomes are broadly considered when selecting controls.</li><li>Controls that aid the effectiveness and efficiency of agency activity are preferred over other controls (assuming similar reduction in risk).</li></ul>	<ul style="list-style-type: none"><li>Corruption control function leads coordination of controls across all three lines.</li></ul>

## Chapter 8: Corruption control framework

While corruption risk management supports the identification of corruption control activity, it is the corruption control framework (“Framework”) that coordinates this activity. In practice, the Framework comprises one or more documents that coordinate corruption control activity.<sup>26</sup> It does this in two ways.

First, a Framework establishes the governance infrastructure for corruption control activity by documenting corruption control assumptions, aims, activities, outputs and outcomes (as per other organisational frameworks). For instance, it might have subheadings relating to the organisational environment, key corruption risks, corruption control activities, and monitoring and evaluating corruption control effectiveness.

Secondly, it coordinates corruption control activity with other systems and processes. This is particularly important because many specialist areas that are associated with corruption control (for example, ethics, legal, governance, risk, ICT security) have their own programs of activities and their own frameworks. Failing to align these frameworks, programs and activities weakens overall control. Similarly, the Framework should have regard to operational activities, such as project management, procurement, and recruitment.

This chapter focuses on general elements of the Framework that can affect its ability to successfully coordinate corruption control. These features either apply to:

- the Framework as a whole
- the corruption control plan (“Plan”) that typically forms part of the Framework.<sup>27</sup>

<sup>26</sup> While the Framework is described here as a document or as documents, it should reflect the agency’s systems. Note that AS 8001:2021 uses the term “fraud and corruption control system”.

<sup>27</sup> Some agencies may have a combined corruption control strategy/plan, rather than a separate Plan.

### Framework features

As with framework implementation in general, better practice corruption control must balance two sometimes competing considerations.

First, the Framework needs to be rigorous in the sense that it incorporates known requirements and better practice principles of corruption control. Failing to incorporate these principles creates the risk of addressing corruption control in an insufficient manner or doing so in a manner that is illegal, unethical or otherwise problematic. For instance, a data analytics program could be implemented in a manner that either fails to search for relevant red flags or searches for those red flags in a manner that breaches privacy or industrial requirements.

Secondly, the Framework needs to be suited to the agency in question. For instance, different agencies face different risk profiles, have different governance arrangements, and different legal and regulatory frameworks. An “off-the-shelf” Framework that fails to acknowledge this runs the risk of being divorced from the on-the-ground operational realities of corruption control.

Key outcomes are that the Framework:

- is rigorous from a corruption control perspective
- ensures that corruption control activity is adapted to an agency’s internal context.

### Corruption control rigour

Together, all the elements of better practice discussed in the previous chapters highlight some general principles to help ensure that Frameworks are rigorous.

Table 24, on page 45, presents how Framework corruption control rigour is implemented for typical cases of Low, Medium and High corruption control maturity.

**Table 24: Corruption control rigour of the Framework**

Maturity	Breadth	Standards and better practice	Reviewed and updated
Low	<ul style="list-style-type: none"><li>• Activity focuses on one line of defence (often Line 2).</li><li>• Organisational associates are ignored.</li></ul>	<ul style="list-style-type: none"><li>• Little consideration of relevant standards or better practice guidance.</li></ul>	<ul style="list-style-type: none"><li>• Framework is reviewed on an ad hoc basis, often only in response to major control breaches.</li></ul>
Medium	<ul style="list-style-type: none"><li>• Activity includes Line 1 and Line 2 activity. Limited Line 3 activity may also be included.</li><li>• There is basic coverage of organisational associates.</li></ul>	<ul style="list-style-type: none"><li>• Framework is guided by relevant standards and better practice guidance.</li></ul>	<ul style="list-style-type: none"><li>• Framework is reviewed at least biennially.</li></ul>
High	<ul style="list-style-type: none"><li>• Applies across all three lines of defence with roles and responsibilities of each clearly specified.</li><li>• Encompasses organisational associates.</li></ul>	<ul style="list-style-type: none"><li>• Systematic review of relevant standards and better practice is conducted, possibly including mapping exercises.</li></ul>	<ul style="list-style-type: none"><li>• As per Medium.</li><li>• Framework is updated in response to changes in the internal and external environment.</li></ul>

## Organisational context

A Framework needs to be tailored to an agency's context. Otherwise, it runs the risk of imposing burdensome controls that are more hypothetical than real. This is particularly the case because, as noted in chapter 1, agencies' operational environments frequently change due to things such as machinery of government changes, resourcing changes, surges in business-as-usual activity and ongoing changes in the risk environment (for example, due to a pandemic or changes in government policy).

Table 25 presents how the Framework is tailored for organisational context for typical cases of Low, Medium and High corruption control maturity.

## Corruption control plan

One of the most important elements of the Framework is the Plan, or equivalent document.<sup>28</sup> The Plan provides an overall direction and cohesion to an agency's corruption control activities.

Key outcomes are that the Plan:

- provides a detailed description of an agency's corruption control efforts
- is tailored to the agency's operational environment.
- corruption risk analysis is discussed in some detail in the "Robustness of corruption risk analysis" section of chapter 7

## Detailed description

Obviously, the ability of a plan to meaningfully guide an agency's corruption control activities is dependent on it containing sufficient detail.

Table 26, on page 47, presents what information is included in Plans for typical cases of Low, Medium and High corruption control maturity.

## Tailoring to the operational environment

Because the Plan references specific risks and controls, it needs to be tailored to the agency's operational environment, including being updated when this environment changes. The key tailoring mechanisms are the extent to which development and update of the Plan is informed by risk analysis, and internal and external consultation.

Maturity tables are not provided regarding this tailoring because relevant maturity information is available elsewhere in the publication namely:

**Table 25: Tailoring of the Framework to organisational context**

Maturity	Integrated with other frameworks	Compliance mechanisms specified
<b>Low</b>	<ul style="list-style-type: none"> <li>• Generic policy statement about the Framework working together with other organisational frameworks.</li> <li>• Framework itemises known, important requirements of legal and regulatory frameworks.</li> </ul>	<ul style="list-style-type: none"> <li>• Framework contains minimal consideration of how compliance with policy and other corruption control requirements will be incentivised.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Key frameworks linked to corruption control are specified in the Framework and vice versa.</li> </ul>	<ul style="list-style-type: none"> <li>• Framework contains general discussion of how agency will incentivise compliance with policy and other corruption control requirements.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Intersection points between the Framework and other frameworks formally mapped to avoid duplication and clashes in planned activities.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Framework explicitly lists key mechanisms used by the organisation to incentivise compliance and disincentivise non-compliance with policy and other corruption control requirements.</li> </ul>

<sup>28</sup> For smaller agencies in particular, the Framework and Plan will be within the same document. In practice, the number of documents is unimportant.

- consultation maturity levels are presented in the “Corruption control specialist” column of table 6 in chapter 4

- maturity levels regarding adapting to changes in the operational environment are presented in the “Reviewed and updated” column of table 24 in this chapter.

**Table 26: Content of plans**

Maturity	Background information	Control activities	Assurance and governance
<b>Low</b>	<ul style="list-style-type: none"> <li>• General information about corruption risks, including possible types of corrupt conduct.</li> </ul>	<ul style="list-style-type: none"> <li>• Lists key corruption control activities.</li> </ul>	<ul style="list-style-type: none"> <li>• No information about reporting on Plan progress or assurance activities.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Lists corruption risks that are most deemed relevant for the agency.</li> <li>• Indicates which parts of the agency are vulnerable to specific corrupt conduct.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Corruption control activities are linked to relevant corruption risks.</li> <li>• Basic information about how each activity is performed (for example, frequency) is included.</li> </ul>	<ul style="list-style-type: none"> <li>• Description of how progress will be reported to senior management and/or governance bodies.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Includes background assumptions behind the Plan (for example, risk appetite, activities performed by organisational associates).</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• All activities are assigned and target completion dates set.</li> <li>• Relevant success measures and data sources are set.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Description of assurance mechanisms to verify implementation of the Plan.</li> </ul>

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to developing a Framework and Plan:

- 2.2 Governing body
- 2.3 Top management
- 2.4 Specialist fraud and corruption control resourcing
- 2.5 Line management
- 2.6 Business unit accountability for fraud and corruption control
- 2.7 Awareness raising of fraud and corruption risk
- 2.8 Fraud and corruption risk management
- 2.9 External environment scan
- 2.10 Developing and implementing a fraud and corruption control system
- 2.13 Information security management system
- 2.14 Recordkeeping and confidentiality of information

## Chapter 9: Corruption control roles

The assignment of corruption control roles is critical to ensure the successful implementation of an agency's corruption control program. For instance, if an agency performs data analysis across its purchase orders as a corruption control activity, specific staff need to be made responsible for running the relevant analytical tests, reviewing the results and determining how to address any red flags.

Corruption control roles should be formally specified as part of the Framework and better practice corruption control involves carefully assigning roles to:

- generalist staff, including frontline managers
- specialist functions
- senior management
- an agency's audit and risk committee (ARC).<sup>29</sup>

### Generalist staff

While it is a truism that “everyone is responsible for corruption control”, corruption control is aided by every staff member understanding what is expected of them. For instance, it is harder for someone to turn a blind eye to corrupt conduct because it is “not their problem” when reporting corrupt conduct has been formally assigned as their responsibility.<sup>30</sup>

<sup>29</sup> NSW local councils use the term “audit, risk and improvement committee” or ARIC. For local government readers, a reference to an ARC in this publication can be read as a reference to an ARIC.

<sup>30</sup> Obviously, these responsibilities, along with any of the other responsibilities and accountabilities discussed in this chapter, need to be communicated to the relevant individuals.

Key outcomes are that all:

- staff are responsible for reporting corrupt conduct, and identifying corruption risks and control weaknesses
- managers are responsible for adopting controls to manage corruption risk within their remit.

Table 27, page on 49, presents responsibilities for generalist staff for typical cases of Low, Medium and High corruption control maturity.

### Specialist functions

There are certain functions that are particularly important from a corruption control perspective. While these functions differ depending on each agency's purpose, design and corruption risk profile, they include any:

- corruption control function, whether or not the individual or unit performing this function also performs other functions
- function that is part of the overall governance of the agency, such as internal audit or enterprise risk (“governance functions”)
- function that owns important anti-corruption controls or vulnerable processes, such as finance, HR, ICT or legal (“process control functions”).

Key outcomes are that:

- there are clear responsibilities for reporting against the Framework<sup>31</sup>
- control of vulnerable processes is informed by expert input

<sup>31</sup> Given the Plan is part of the Framework, responsibilities for reporting against the plan are included here.



- the types of controls discussed in chapters 3–6 are designed and implemented effectively and efficiently.

Table 28, on page 50, presents responsibilities for specialist functions for typical cases of Low, Medium and High corruption control maturity.

**Table 27: Responsibilities of generalist staff**

Maturity	All staff	Frontline managers
<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• No specific responsibilities assigned but there is a general statement that everyone has a role in preventing and detecting corrupt conduct.</li> </ul>	<ul style="list-style-type: none"> <li>• Considering and implementing corruption controls recommended by Line 2 and Line 3.</li> </ul>
<ul style="list-style-type: none"> <li>• Medium</li> </ul>	<ul style="list-style-type: none"> <li>• Reporting known corrupt conduct.</li> <li>• May be encouraged to report corruption risks but no formal responsibility is assigned.</li> </ul>	<ul style="list-style-type: none"> <li>• Implementing controls to manage corruption risks in their area.</li> <li>• Modelling ethical behaviour for their subordinates and raising awareness of corruption control issues.</li> </ul>
<ul style="list-style-type: none"> <li>• High</li> </ul>	<ul style="list-style-type: none"> <li>• Reporting all integrity issues including reasonably suspected corrupt conduct.</li> <li>• Identifying corruption risks and control weaknesses that apply to their work.</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Managing corruption risks linked to relevant organisational associates.</li> <li>• Ensuring subordinates have the knowledge and skills to fulfil their corruption control responsibilities.</li> <li>• Obtaining assurance that corruption controls they implement are working effectively.</li> </ul>

**Table 28: Responsibilities of specialist functions**

Maturity	Corruption control function	Governance functions	Process control functions
Low	<ul style="list-style-type: none"> <li>Reporting against the Framework.</li> </ul>	<ul style="list-style-type: none"> <li>Reporting any potential corruption vulnerabilities their work identifies.</li> </ul>	<ul style="list-style-type: none"> <li>Implementing corruption controls assigned to them.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Helping process control functions to design and implement corruption controls.</li> <li>Providing input on how vulnerable systems and processes can be adequately controlled.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Including vulnerable systems and processes in organisational assurance activities.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Designing corruption controls regarding their processes.</li> <li>Demonstrating that adequate controls have been adopted to protect vulnerable systems and processes.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Coordinating the agency's corruption control program.</li> <li>Obtaining assurance that corruption control activities have been performed appropriately.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Providing assurance about the adequate operation of specific corruption controls.</li> <li>Providing assurance about the adequate operation of the Framework in general.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Verifying that corruption controls regarding their processes are working as intended.</li> </ul>

## Senior management accountabilities

While accountabilities for specific corruption control activities are logically assigned according to organisational hierarchy, broad accountabilities for an agency's corruption control program cannot be so easily assigned because they relate to activity across the whole organisation.

Key outcomes are that:

- corruption control activities receive sufficient organisational support and resourcing
- corruption control is integrated with other organisational activity
- senior management can readily hold an individual accountable for the agency's corruption control program.

Table 29, on page 51, presents senior management accountabilities for typical cases of Low, Medium and High corruption control maturity.

## Audit and risk committee

An agency's ARC plays a key role in its governance, and better practice corruption control includes the integration of corruption risk management with broader risk management efforts. Consequently, better practice corruption control assigns an agency's ARC a role to oversee its corruption control program.

As discussed in a relevant Commission publication<sup>32</sup>, the ARC's role does not involve overseeing day-to-day corruption control activity, such as getting involved in individual complaints or investigations. Instead, it involves overseeing the broader functioning of an agency's corruption control program.

Key outcomes are that:

- the agency has assurance that its Framework represents better practice
- corruption control functions are performed in accordance with better practice

<sup>32</sup> NSW ICAC, *Dealing with Corruption, Fraud and the ICAC: the role of public sector Audit and Risk Committees*, Sydney, September 2020.

- activities of other governance functions (for example, internal audit, risk management) sufficiently consider potential corrupt conduct.

Table 30, on page 52, presents an ARC's corruption control role for typical cases of Low, Medium and High corruption control maturity.

**Table 29: Accountabilities of senior management**

Maturity	Organisational support	Integration with other work	Corruption control program
Low	<ul style="list-style-type: none"> <li>Statement exists about the agency supporting corruption control (including PID Act compliance) but no accountabilities assigned to senior management.</li> </ul>	<ul style="list-style-type: none"> <li>No accountabilities assigned to senior management to integrate corruption control with other organisational activity.</li> </ul>	<ul style="list-style-type: none"> <li>Unclear or unspecified accountability for operation of corruption control program.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Promoting integrity throughout agency.</li> <li>Adequately resourcing corruption control.</li> <li>Promoting a positive reporting culture which encourages and supports staff to report wrongdoing under the PID Act.</li> </ul>	<ul style="list-style-type: none"> <li>Integrating corruption risk management with broader risk management efforts.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability for operation of corruption control program more than two levels removed from agency head.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Ensuring corruption control is not adversely impacted by a lack of authority or information flow.</li> <li>Providing governance over corruption control, including monitoring risk mitigation efforts and control-related reports. Ensuring that PID risk assessments are conducted.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Integrating the Framework with other frameworks such as those for organisational performance management, enterprise risk management and assurance.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability for operation of corruption control program no more than two levels removed from agency head.</li> </ul>

**Table 30: Role of ARCs**

Maturity	Assurance regarding framework	Corruption control functions	Assurance coverage
Low	<ul style="list-style-type: none"> <li>Receives a copy of the updated Framework.</li> </ul>	<ul style="list-style-type: none"> <li>Receives output-based reports on corruption control functions.</li> </ul>	<ul style="list-style-type: none"> <li>Treats corruption control as completely separate to risk management and internal audit.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Provides input into the Framework review process.</li> <li>Asks questions about adequacy of the Framework.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Receives basic trend analysis on corruption control topics.<sup>33</sup></li> <li>Obtains assurance that legislative requirements regarding corruption control activity are met.<sup>34</sup></li> <li>Advised of key lessons learnt from sources of better practice, potential corrupt conduct and near-miss incidents.</li> </ul>	<ul style="list-style-type: none"> <li>Obtains assurance that corruption risks are included in the enterprise risk register.</li> <li>Obtains assurance that internal audit considers corruption vulnerabilities when conducting audits.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Obtains assurance that the Framework is informed by and embodies better practice.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Receives detailed<sup>35</sup> trend analysis on corruption control topics.</li> <li>Obtains assurance that corruption control units are performing their functions adequately.</li> <li>Obtains assurance that lessons learnt from sources of better practice, potential corrupt conduct and near-miss incidents are put in practice.</li> </ul>	<ul style="list-style-type: none"> <li>Obtains assurance that corruption risks are <i>sufficiently</i> included in the enterprise risk register.</li> <li>Obtains assurance that corruption risks are considered in the internal audit program.</li> </ul>

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to determining and assigning corruption control roles:

- 2.3 Top management
- 2.4 Specialist fraud and corruption control function
- 2.5 Line management
- 2.11 Leveraging the internal audit function in fraud and corruption control
- 2.12 Leveraging the external audit function in fraud and corruption control

<sup>33</sup> For example, allegations, investigations, probity issues, gifts and benefits, conflicts of interest.

<sup>34</sup> For instance, compliance with the PID Act.

<sup>35</sup> The distinction between basic and detailed trend analysis often is in terms of both the number and complexity of analyses.

This page is intentionally blank.

## Chapter 10: Corruption control competence

The day-to-day operation of many corruption controls is dependent on the competence of the people who implement them. Staff and organisational associates may provide training on ethical issues, identify organisational performance issues, make complaints alleging corrupt conduct and conduct investigations. If these individuals are not sufficiently capable, the effectiveness of these controls is reduced.

While many aspects of corruption control rely on general analytical and organisational skills, some specialist knowledge is also required to successfully implement corruption control mechanisms. This publication terms this knowledge “corruption control competence”.

The requirements for corruption control competence differ depending on an individual’s position, although broad similarities can be drawn across:

- generalist positions, although additional knowledge is needed for individuals involved in governance, assurance or compliance activities
- specialist corruption control positions.

### Generalists

Generalists are staff or organisational associates who are not in a specialist corruption control role. The corruption control competence generalists require is essentially the baseline competence required across the whole agency.

This baseline differs for non-managerial staff, managers and organisational associates because each of them has different corruption control roles (see chapter 9). For a similar reason, additional corruption control knowledge is needed for individuals involved in governance, assurance or compliance activities.

Better practice corruption control achieves the following outcomes:

- Knowledge of corruption control-related policies is sufficient to ensure that ignorance is not a valid excuse for not following them.
- The ability to identify likely corruption risks and prudent control strategies.
- Staff and organisational associates know how to respond to suspected corrupt conduct.

### Policy knowledge

From a corruption control perspective, there are certain policies within an agency’s policy framework that are particularly important because they embed critical controls. These are either:

- key ethics or probity policies (for example, gifts and benefits, conflicts of interest and reporting misconduct policies)
- policies regarding functions that are both performed frequently and are high risk for corruption, such as procurement and recruitment policies.

An important element of generalist corruption control competence is knowledge of these policies, including how to implement them. Obviously, this can only be done if the agency establishes a clear listing of all such policies and maps intersection points between them.

Table 31, on page 55, presents knowledge of corruption control-related policies for typical cases of Low, Medium and High corruption control maturity.

**Table 31: Corruption control-related policy knowledge**

Maturity	Non-manager	Manager	Organisational associate
Low	<ul style="list-style-type: none"><li>• Aware of corruption control-related policies.</li></ul>	<ul style="list-style-type: none"><li>• Aware of corruption control-related policies. Knows general policy requirements.</li></ul>	<ul style="list-style-type: none"><li>• Aware that agency has corruption control-related policies that might apply to them.</li></ul>
Medium	<ul style="list-style-type: none"><li>• As per Low.</li><li>• Knows general policy requirements.</li><li>• Understands relevance of policies to situations they encounter.</li></ul>	<ul style="list-style-type: none"><li>• Knows specific requirements that relate to their team's day-to-day duties.</li><li>• Able to consistently apply these requirements.</li></ul>	<ul style="list-style-type: none"><li>• Knows which of the agency's corruption control-related policies apply to them.</li></ul>
High	<ul style="list-style-type: none"><li>• As per Medium.</li><li>• Able to consistently apply policies even in complex or "grey" situations.</li></ul>	<ul style="list-style-type: none"><li>• As per Medium.</li><li>• Has a good general understanding of policy requirements that are not applicable to their team's day-to-day duties.</li></ul>	<ul style="list-style-type: none"><li>• As per Medium.</li><li>• Knows key requirements within policies.</li><li>• Aware of key policies that apply to agency staff with whom they deal.</li></ul>



## Corruption risk knowledge

An agency's ability to manage corruption risks is dependent on its staff and organisational associates understanding those risks. For instance, a risk workshop is unlikely to produce an accurate analysis if attendees have a limited understanding of the nature of corruption risk.

Consequently, one element of generalist corruption control competence is an understanding of corruption risk

management concepts (which, in turn, requires a general understanding of risk management).

Table 32 presents the understanding of corruption risk management concepts for typical cases of Low, Medium and High corruption control maturity.

**Table 32: Corruption risk knowledge**

Maturity	Non-manager	Manager	Organisational associate
<b>Low</b>	<ul style="list-style-type: none"> <li>Understands that their work could be impacted by corrupt conduct.</li> </ul>	<ul style="list-style-type: none"> <li>Has a general understanding of corruption risks and controls, including how they might broadly apply to their remit.</li> </ul>	<ul style="list-style-type: none"> <li>Understands that they could act corruptly or be subject to corrupt conduct committed by the agency's staff.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Understands relevant corruption risks and vulnerabilities.</li> </ul>	<ul style="list-style-type: none"> <li>Understands that corruption risks and applicable controls differ across units, functions and activities.</li> <li>Knows the risks and controls applicable to their remit.</li> <li>Has a general understanding of other corruption risks and controls.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Understands likely ways in which their potential actions could constitute corrupt conduct and likely ways that a staff member might engage in corrupt conduct.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Understands how things such as waste, non-compliance, poor performance and inadequate processes create corruption opportunities.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Understands that corruption is an operational risk and corruption control is about day-to-day practice.</li> <li>Recognises that decreases in performance or quality could indicate corruption.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Is aware of controls that could be adopted to manage relevant corruption risks.</li> </ul>

## Response to suspected corrupt conduct

As discussed in chapter 5, complaints by knowledgeable insiders such as staff and organisational associates is the most frequent means by which corrupt conduct is detected.

However, a functioning complaints management system relies on people knowing how to respond to suspected corrupt conduct. For instance, a well-meaning but

uninformed individual might launch their own enquiries or confront the alleged perpetrator instead of using a designated reporting channel. Such actions can ultimately create a range of negative impacts for an agency, such as legal or industrial issues, accidentally tipping off alleged perpetrators or the destruction of evidence.

Table 33 presents knowledge of how to respond to suspected corrupt conduct for typical cases of Low, Medium and High corruption control maturity.

**Table 33: Knowledge of how to respond to corrupt conduct**

Maturity	Non-manager	Manager	Organisational associate
<b>Low</b>	<ul style="list-style-type: none"> <li>Aware that suspected corrupt conduct can be reported internally or externally.</li> </ul>	<ul style="list-style-type: none"> <li>Knows how suspected corrupt conduct can be reported internally and externally.</li> </ul>	<ul style="list-style-type: none"> <li>Aware that the agency takes allegations of corrupt conduct very seriously.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>Knows how suspected corrupt conduct can be reported internally and externally.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Has broad familiarity with PID requirements and internal PID processes.</li> </ul>	<ul style="list-style-type: none"> <li>Knows relevant internal and external channels for reporting suspected corrupt conduct.</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Has broad familiarity with PID requirements and internal PID processes.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Has sufficient knowledge to comply with PID Act when receiving or managing PIDs.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Aware of any differences or limitations regarding using these channels that apply to them as opposed to staff, including the potential applicability of the PID Act.</li> </ul>

## Governance, assurance and compliance activities

Governance, assurance and compliance activities are an important part of corruption control, so individuals conducting these activities need additional knowledge to ensure these activities adequately contribute to an agency's corruption control program.

Table 34 presents additional corruption control-related policy and corruption risk knowledge needed by individuals performing these activities for typical cases of Low, Medium and High corruption control maturity. These individuals do not require any additional knowledge about how to respond to corrupt conduct, unless they are involved in activities such as complaint management or investigations.

## Corruption control specialists

Specialists need to have a more detailed understanding of corruption control considerations than generalists. This is because, as discussed in chapter 9, they have technical corruption control responsibilities.

Key outcomes are that specialists:

- ensure that corruption control activity is based on input from both corruption control and process experts; given this has been discussed elsewhere in this publication (for example, the "Corruption control specialist" column of table 6 in chapter 4) it is not included in the maturity table below
- use psychological understanding of the causes of corrupt behaviour and its mitigation to inform corruption control activity
- use performance and benchmarking data to guide and monitor corruption control activity
- have the capacity to diagnose and remedy corruption control weaknesses.

Table 35, on page 59, presents corruption control specialist understanding for typical cases of Low, Medium and high corruption control maturity.

**Table 34: Additional knowledge required for governance, assurance and compliance activities**

Maturity	Corruption control policies	Corruption risk
<b>Low</b>	<ul style="list-style-type: none"> <li>• Broad knowledge of links between specific corrupt conduct and specific policies (for example, gifts are often linked to favouritism).</li> </ul>	<ul style="list-style-type: none"> <li>• Aware that corrupt conduct is usually associated with other organisational issues, such as poor performance and non-compliance.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• Detailed knowledge of how specific corrupt conduct and specific policies are linked (for example, gifts can be used to groom public officials, leading to capture and ultimately favouritism).</li> </ul>	<ul style="list-style-type: none"> <li>• As per Low.</li> <li>• Understands how these issues can provide a cover for corrupt conduct and how examining them in more detail may detect potential corrupt conduct.<sup>36</sup></li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Understands the agency's particular compliance challenges (for example, free events are often offered to staff).</li> </ul>	<ul style="list-style-type: none"> <li>• As per Medium.</li> <li>• Has detailed knowledge of relevant red flags of corrupt conduct and how to further examine them to detect potential corrupt conduct.</li> </ul>

<sup>36</sup> Although this might be done by others, they need to know what can be done, not necessarily be able to do it themselves. (This also applies to the second dot point in the High maturity column.)

**Table 35: Corruption control specialist understanding**

Maturity	Psychological understanding	Performance and benchmarking	Corruption vulnerabilities
Low	<ul style="list-style-type: none"> <li>Aware that corrupt behaviour arises from a combination of situational and individual factors.</li> </ul>	<ul style="list-style-type: none"> <li>Understands the value of monitoring trends in alleged corrupt conduct.</li> </ul>	<ul style="list-style-type: none"> <li>Can identify and remedy corruption control failings following corrupt conduct or a near miss incident.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Familiar with psychological models used to explain corrupt behaviour (for example, fraud triangle, routine activity theory).</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Understands value of monitoring trends in the functioning of corruption controls.</li> </ul>	<ul style="list-style-type: none"> <li>As per Low.</li> <li>Can take general corruption control guidance and tailor it to the agency to identify and remedy corruption control weaknesses.</li> </ul>
High	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Familiar with psychological factors relevant to reporting corrupt conduct (for example, the bystander effect) and poor corruption risk management (for example, risk perception biases).</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Understands the value of monitoring general performance or quality metrics.</li> <li>Has the capacity to conduct benchmarking exercises involving monitored data.</li> </ul>	<ul style="list-style-type: none"> <li>As per Medium.</li> <li>Able to analyse agency systems and processes to diagnose and remedy corruption control weaknesses without reference to corruption control guidance.</li> </ul>

## Relevant Australian Standard sections

The following Australian Standard sections are relevant to determining and assigning corruption control roles:

- 2.3 Top management
- 2.4 Specialist fraud and corruption control resourcing
- 2.5 Line management
- 2.6 Business unit accountability for fraud and corruption control
- 2.7 Awareness raising of fraud and corruption risk
- 2.8 Fraud and corruption risk management
- 2.9 External environment scan
- 2.10 Developing and implementing a fraud and corruption control system
- 4.6 Fraud and corruption reporting channels
- 4.7 Whistleblower management systems
- 4.8 Leveraging relationships with business associates and other external parties
- 4.9 Complaint management







INDEPENDENT COMMISSION  
AGAINST CORRUPTION  
NEW SOUTH WALES

Level 7, 255 Elizabeth Street  
Sydney NSW 2000 Australia

**Postal address:** GPO Box 500  
Sydney NSW 2001 Australia

**T:** 02 8281 5999

**Toll free:** 1800 463 909 (for callers outside metropolitan Sydney)

National Relay Service users: ask for 02 8281 5999

**F:** 02 9264 5364

**E:** [icac@icac.nsw.gov.au](mailto:icac@icac.nsw.gov.au)

**[www.icac.nsw.gov.au](http://www.icac.nsw.gov.au)**

**Business hours:** 9 am to 5 pm, Monday to Friday