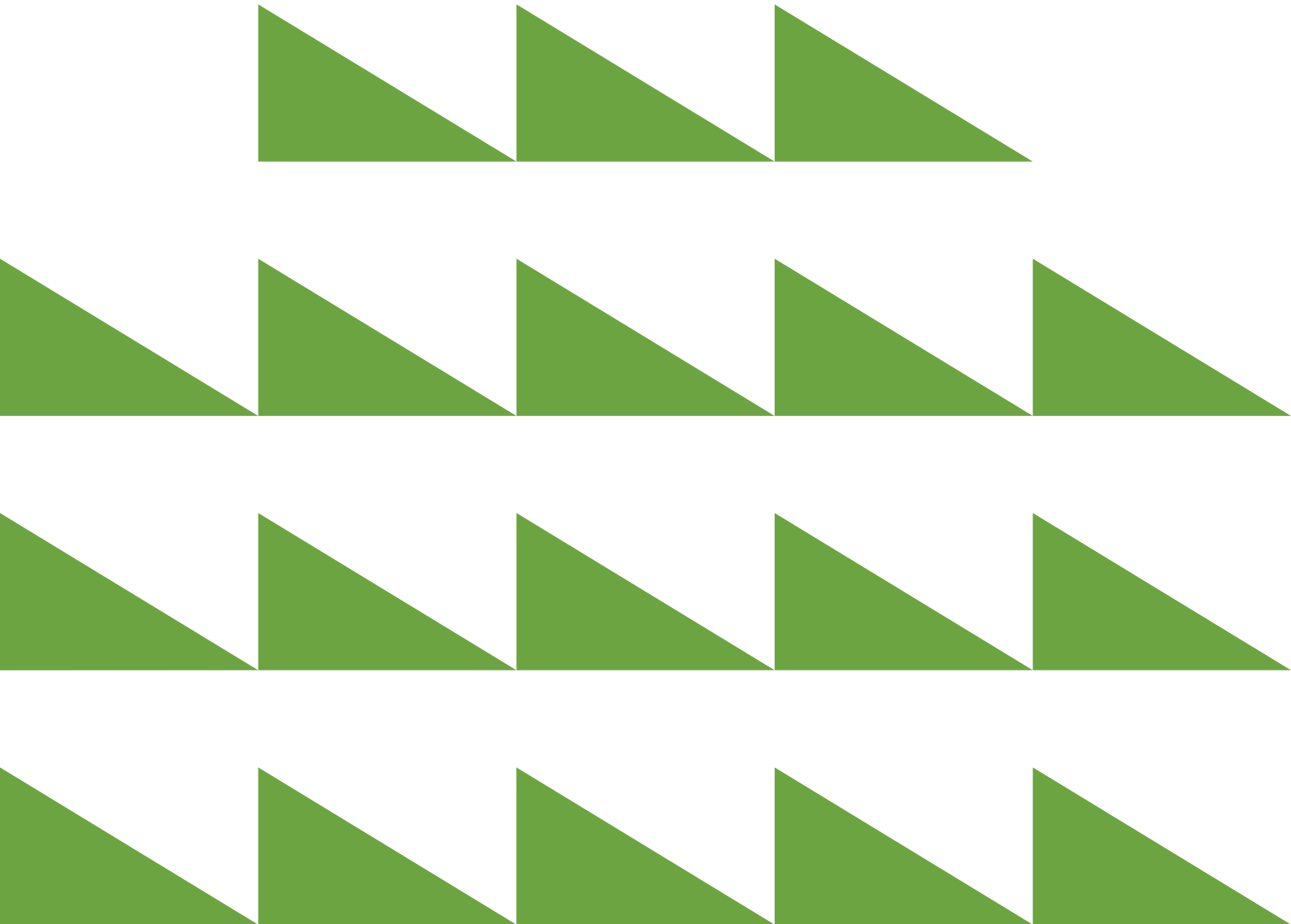
ibac independent broad-based anti-corruption commission
Victoria

State government integrity frameworks review

June 2019



Authorised and published by the
Independent Broad-based Anti-corruption Commission,
Level 1, 459 Collins Street, Melbourne.

June 2019

If you need this information in an accessible format, please call 1300 735 135 or email communications@ibac.vic.gov.au.

This document may also be found in formats on our website www.ibac.vic.gov.au

ISBN 978-0-6482993-4-9 (print)

ISBN 978-0-6482993-5-6 (online)

Contents

Definitions

Acronym/Term	Explanation
CenITex	CenITex provides centralised ICT support to state government departments and agencies
CEO	Chief Executive Officer
FAQs	Frequently asked questions
FTE	Full-time equivalent
IBAC	Independent Broad-based Anti-corruption Commission
IBAC Act	*Independent Broad-based Anti-corruption Commission Act 2011*
KPIs	Key performance indicators
NSW ICAC	New South Wales Independent Commission Against Corruption
PD Act	*Protected Disclosure Act 2012*
PID	Public interest disclosure
PwC	PricewaterhouseCoopers Consulting (Australia) Pty Limited
RFQ	Request for quote
RFT	Request for tender
VAGO	Victorian Auditor-General's Office
VGPB	Victorian Government Purchasing Board
VMIA	Victorian Managed Insurance Authority
VO	Victorian Ombudsman
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VPS	Victorian Public Service
VPSC	Victorian Public Sector Commission
VPS Code of Conduct	Code of Conduct for Victorian Public Sector Employees
WA Health	Department of Health, Western Australia
WA CCC	Western Australian Corruption and Crime Commission

1 Overview

This report provides an overview of integrity frameworks examined in 38 Victorian state government agencies in 2018. A key objective of the review was to help state government agencies review and strengthen their own integrity frameworks, to improve their capacity to prevent corrupt conduct.[1]

Corruption in state government agencies can lead to the loss of public resources, reduction in economic development and diminished community trust which can have implications for public safety and the delivery of important programs and services.

Victorian state government agencies are responsible for a wide range of public services and infrastructure. These agencies vary in size and functions. Their responsibilities include the delivery of key community services, the management of public facilities and natural resources, and regulatory functions. All these activities must be conducted in a manner that ensures public funds are appropriately used in the public interest and to the benefit of the Victorian community.

Given the resources and responsibilities entrusted to state government agencies, it is important they develop, implement and maintain effective integrity frameworks, and continuously improve their capacity to identify and prevent corrupt conduct.

This review of integrity frameworks in state government agencies identified a number of initiatives the broader public sector could consider to strengthen their own integrity frameworks, including the application of more robust due diligence processes for suppliers, development of more interactive training in corruption prevention awareness, and consideration of integrity-related performance measures.

The review also suggests agencies are developing a greater awareness of potential corruption risks, exploring new detection and prevention mechanisms as they become available, and fostering a culture of integrity.

IBAC invited 50 Victorian state government agencies to participate in this review. Thirty-eight agencies agreed to participate.

In 2018, IBAC engaged PricewaterhouseCoopers Consulting (Australia) Pty Limited (PwC) to conduct an analysis of the survey responses provided by the 38 Victorian state government agencies in relation to their integrity frameworks.[2]

[1] In March 2019 IBAC published its *Local government integrity frameworks review*, which provides a snapshot of the integrity frameworks examined in a sample of six Victorian councils. The report highlighted examples of good practices and possible areas for improvement in the local government sector.

[2] PwC conducted an analysis of the survey responses solely for IBAC's use and benefit in accordance with and for the purpose set out in its engagement letter with IBAC dated 22 January 2018. In doing so, PwC acted exclusively for IBAC and considered no-one else's interests. PwC accepts no responsibility, duty or liability to anyone other than IBAC in connection with the analysis of the survey responses; or IBAC for the consequences of using or relying on the analysis of the survey responses for a purpose other than that referred to above. PwC makes no representation concerning the appropriateness of the IBAC report for anyone other than IBAC. If anyone other than IBAC chooses to use or rely on it, they do so at their own risk. This disclaimer applies to the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute.

This review builds on earlier work published by IBAC including:

- a 2014 review of integrity frameworks in Victorian state government agencies (the 2014 review)[3]
- a 2017 survey of Victorian state government employees and their perceptions of corruption (the 2017 survey of state government employees)[4]
- a 2016 guideline on protected disclosures.[5]

Three tiers of agencies

For the purposes of this review, the 38 participating agencies were grouped into three tiers:

- Tier 1 included 13 agencies with fewer than 300 full-time equivalent (FTE) employees. The agencies in this group were split reasonably evenly between those that perform regulatory functions, those that provide services and those that manage natural resources and/or public facilities. These agencies tended to have an annual income of less than $80 million.[6]
- Tier 2 included 18 agencies with 300 to 11,000 FTE employees. Most of these agencies provide services or manage natural resources and/or public facilities. They tended to have an annual income of $80 million to $2 billion.
- Tier 3 comprised the seven state government departments.[7]

This breakdown is broadly consistent with the 2014 review, however the two tiers comprising the smallest agencies in the first review were condensed into Tier 1 in this analysis.

Structure of this report

This report outlines observations and findings from the current review about risk management, ethical culture and leadership, and detection of suspected instances of corrupt conduct, with reference to guidance in the Australian Standard AS 8001-2008 'Fraud and Corruption Control' (the Standard) in relevant sections.

This report also discusses the integrity framework information and documentation provided by participating agencies, as well as case studies and examples identified during the analysis of survey response data and consultations.

Where relevant, differences observed between the 2014 and 2019 reviews are discussed.

Finally, the report includes observations regarding better practice and possible enhancements to existing policies and procedures in risk management, ethical culture and leadership, and detection to inform the broader public sector and help them tailor strategies that are relevant and applicable to an individual agency's circumstances.

The importance of integrity frameworks

An integrity framework brings together the instruments, processes, structures and conditions required to foster integrity and prevent corruption in public organisations.[8]

For the purposes of this report, integrity frameworks should include robust risk management processes, and fraud and corruption control frameworks to identify and address corruption risks. They should also encompass governance and leadership, deterrent and prevention measures, detection mechanisms, and communication and training to promote awareness and understanding of an agency's integrity principles and initiatives.

In this review, participating agencies' policy documents and survey responses were broadly assessed against the Standard which sets out key elements of an effective fraud and corruption control framework. The Standard identifies the implementation and maintenance of an integrity framework as a key element of fraud and corruption control.

[3] IBAC 2014, *A review of integrity frameworks in Victorian public sector agencies*, Melbourne.

[4] IBAC 2017, *Perceptions of corruption: Survey of Victorian state government employees*, Melbourne.

[5] IBAC 2016, *Guidelines for making and handling protected disclosures and Guidelines for protected disclosure welfare management*, Melbourne.

[6] Income refers to an agency's total annual income from transactions, as reported in their most recent annual report prior to the commencement of the review.

[7] There were seven departments at the time of this review.

[8] Based on the definition developed by the Organisation for Economic Co-operation and Development, Integrity Framework, www.oecd.org/gov/44462729.pdf.

According to the Standard, an integrity framework should include:

- Example setting: Senior managers should lead by example, by modelling expected standards of behaviour and complying with the various elements of the organisation's integrity framework.
- Senior management recognition: Senior managers should recognise and regularly promote the importance of an ethical culture.
- Reporting of complaints: It is critical organisations have a clear mechanism to report ethical concerns regarding the organisation, both for external and internal complaints.
- Codes of behaviour: Organisations should implement codes of conduct that include a high-level aspirational statement of values and more prescriptive actions to support a culture of integrity.
- Allocation of responsibility: A senior officer should have clear responsibility for ensuring the organisation's integrity initiatives are implemented and monitored.
- Ethics committee endorsement: There is value in a committee or dedicated forum providing authoritative advice on integrity issues that cannot be resolved by a line manager.
- Communication: There should be a program for regularly communicating the organisation's code of conduct.
- Training: It is important to provide specific, ongoing training on the code of conduct, and fraud and corruption awareness.
- Performance management reinforcement: There is value in incorporating ethical standards in performance assessment systems, remuneration strategies, and employee feedback.
- Benchmarking: Analysis of ethical standards over time can help identify improvement in an organisation's integrity standards.
- Compliance: Organisations may require all employees to sign an annual declaration that they have complied with integrity policies including those concerned with conflict of interest, disclosure of information and other integrity-related matters.

This review indicates participating agencies have developed integrity frameworks that address these key elements, although with varying levels of maturity. Consistent with regulatory requirements (see 2.1.2), the integrity framework policies provided by agencies generally included a fraud and corruption control plan and policy, code of conduct, conflict of interest policy, gifts and benefits policy, supplier engagement policy, and protected disclosure procedures. Agencies reported that during the development and review of their frameworks, reference was made to the Standard as well as information from other Victorian public sector agencies, including IBAC and interstate anti-corruption agencies.

1.1 Key findings

This review of integrity frameworks in 38 Victorian state government agencies was undertaken in three stages involving an organisational integrity framework survey, a review of agency policies and procedures, and in-depth consultations with a sample of 10 participating agencies to explore specific issues.

Outlined below are the key findings of the review.

1.1.1 Fraud and corruption control

A fraud and corruption control plan should document an agency's approach to controlling fraud and corruption risks, and identify action the agency intends to take to implement and monitor initiatives to prevent, detect and respond to fraud and corruption.

A control plan can also help to consolidate fraud and corruption control resources, ensure a consistent approach across the organisation, and identify whether further work or additional resources are required. Agencies should view their fraud and corruption control plan as a vehicle to guide the development and coordination of other fraud and corruption control activities.

Most agencies across all three tiers provided evidence of a fraud and corruption control plan. The information provided indicated these plans are regularly reviewed and amended at two to three-year intervals, and when a significant change in business conditions or practices is identified. The research also indicated agencies across all tiers were generally aware of the importance of developing a control plan, and considered it a key part of their corruption risk management.

1.1.2 Assessment of corruption risks

Agencies should have policies and processes in place to systematically identify, analyse and evaluate their most significant fraud and corruption risks, and what controls can mitigate those risks.

IBAC's 2014 review of state government agencies' integrity frameworks observed that while most participating agencies reported having risk assessment processes related to financial, audit or fraud risks, very few reported conducting specific corruption risk assessments. Accordingly, the risks most commonly identified by agencies in the earlier review related to financial management or procurement and the integrity of the agency's information technology or information security, but not to specific corruption risks. As such, the 2014 review concluded 'corruption and its prevention is generally not on the radar of Victorian public sector agencies'.[9]

In the 2019 review, agencies were presented with a list of potential corruption risks and asked to indicate the extent to which each posed a corruption risk to the agency, whether the risk was recorded on the agency's risk register, and whether any controls were in place to manage that risk. The issues commonly identified by most participating agencies as posing a corruption risk to their organisation were improper procurement (36 agencies), conflict of interest (35) and misuse of information or material (35).

Responses also indicated most participating agencies formally record corruption risk issues in their risk registers and implement controls to mitigate those risks. Conflicts of interest, improper procurement, and improper cash handling or payment arrangements were the issues most frequently controlled for and recorded on risk registers.

These results suggest that while agencies are now cognisant of a broader range of corruption risks, financial and fraud-related corruption risks continue to receive more attention.

[9] IBAC 2014, *A review of integrity frameworks in Victorian public sector agencies*, Melbourne, p 2.

1.1.3 Ethical culture and leadership

Senior management commitment to controlling the risk of fraud and corruption was generally well covered in the documentation provided by agencies. Policies included statements of commitment to the implementation and oversight of integrity initiatives, and strong messaging that senior management is ultimately responsible for promoting a culture of compliance in this area. Fraud and corruption control policies and codes of conduct detailed the roles and responsibilities of each level of leadership and line management.

Many agencies also had dedicated fraud and corruption teams in the form of panels, forums, and/or decision-making boards to provide oversight to the organisation's integrity framework, and benchmark its ethical standards.

1.1.4 Training and other initiatives to promote integrity and awareness of corruption risks

Education and training provided by agencies to employees about corruption awareness and prevention appears to have increased in frequency and scope since the 2014 review. Since becoming fully operational in 2013, IBAC has undertaken a number of investigations in the public sector. These may have contributed to an increased focus on the need for corruption prevention education and training.

IBAC's 2014 review noted relatively few participating agencies reported having specific education or training programs for staff to help them understand what constitutes corruption. Content for such training was generally limited to the Code of Conduct for Victorian Public Sector Employees. At the time, it was noted that this document contained very little specific information about corruption.

The current review found most participating agencies now provide dedicated corruption and integrity training, or integrate this content into other training. Content is tailored to the audience, with certain higher risk roles receiving additional, more focused training.

In addition to education and training programs, agencies were asked to discuss initiatives they used to promote integrity in their organisations. Innovative approaches identified included:

- risk champions or other designated individuals within the agency with a specific role or responsibility to promote risk awareness, support business units and report to senior management
- organisational support for specific committees or forums dedicated to risk and/or integrity matters coupled with endorsement of integrity-related policy and program improvements
- leadership responding, and being seen to respond appropriately, when integrity issues are raised
- communication by way of training, newsletters, emails, intranet and noticeboard posts
- the inclusion of integrity criteria in position descriptions and performance plans
- employee declarations of compliance with policies.

1.1.5 Assurance that integrity is promoted and understood

Across all participating agencies, the top three ways in which senior management assures itself integrity is promoted, and employees have a good understanding and confidence in corruption prevention are:

- leading by example
- training
- support for audits and other reviews that monitor compliance with integrity framework policies.

The main purpose of training and other initiatives to promote integrity and understanding of corruption risks is to raise awareness so employees are better equipped to identify potential fraud and corruption, ensure they know how to report suspected corrupt conduct, and have confidence the agency supports people who speak up.

It can be helpful to test awareness through staff surveys and other feedback mechanisms. Insight into staff awareness of fraud and corruption risks, as well as compliance with an agency's internal controls, can help identify staff concerns and misconceptions that may need to be addressed through integrity and corruption awareness initiatives.

1.1.6 Detection

An integrity framework must include mechanisms to help state government agencies detect corrupt conduct in a timely manner. Employees need to know how to report suspected corrupt conduct, and have confidence in reporting mechanisms. It is also critical that agencies undertake proactive auditing to identify potential corruption risk areas within their organisation.

Responses to the review suggest communication and awareness about reporting avenues have improved since the 2014 review. Most participating agencies provided policy documents which indicated they had reporting mechanisms, and procedures in place to handle complaints and protected disclosures.

Understanding of protected disclosures was demonstrated across all three tiers of agencies, regardless of whether an agency could receive protected disclosures directly. For the most part, there was a clear understanding of what constitutes a protected disclosure, the role of a protected disclosure coordinator, when matters should be escalated, and when to refer a matter to IBAC.

The main ways agencies identified suspected corrupt conduct was through identification or reporting by colleagues, and by identification and/or reporting by supervisors and managers.

Across all three tiers, most agencies indicated staff are encouraged to report suspected fraud and corruption to a senior staff member. However, few provided specific examples of how this was achieved.

1.1.6.1 Data analytics

The review indicated some agencies have adopted innovative approaches to detection of suspected fraud and corruption using data analytics. Other agencies indicated they were aware of the value of data analytics to detect potential corrupt conduct.

In consultations, one department advised that three employees work full-time on compliance reviews and conduct a monthly reconciliation of corporate cards. That process involves examining expenses data to identify unusual amounts or suspect purchases, which can help detect policy breaches. The finance team also uses analytics to check transactions related to accommodation, flowers, restaurants, and duplicate payments - especially expenses incurred om weekends.

Data analytics can be used to detect and prevent fraudulent and corrupt conduct, including by identifying early warning signs of potential integrity breaches, understanding trends that might be associated with high-risk issues, and monitoring the effectiveness of controls. To use data analytics most effectively, agencies need to have identified their areas of highest risk and collect information in a way that facilitates analysis.

1.1.7 Knowledge and perceptions of IBAC

Most participating agencies indicated they were aware of IBAC and its corruption prevention work. This was consistent with the 2014 review.

A number of agencies noted they had sought advice and insights from IBAC including making general or specific enquiries, and attending information presentations. Agencies noted they would not look to IBAC for advice regarding integrity policies, procedures, or learning and development related to integrity in the first instance. However, several agencies noted they had sought guidance from IBAC when preparing their protected disclosure and other reporting-related policies.

Agencies also said they found case studies and real life examples highlighting corruption risks, effective controls and investigation outcomes to be useful.

2 Background and methodology

2.1 Background to this review

2.1.1 Previous IBAC research

In 2013, IBAC commissioned a review of Victorian state government integrity frameworks, which provided baseline information on systems and practices used to detect and prevent corruption in a sample of public sector agencies in Victoria (the 2014 review).[10] The methodology for the 2019 review is based on the approach adopted for the 2014 review.

The 2014 review found corruption and its prevention were not generally on the radar of the participating agencies. Most reporting systems or complaints mechanisms focused on suspected fraud rather than suspected corruption, making it difficult for agencies to be alert to and respond to corruption risks. There was also little evidence of senior management having oversight of corruption prevention measures.

The 2019 review considered the integrity frameworks of a different sample of Victorian state government agencies to identify:

- strengths and weaknesses in a sample of state government integrity frameworks
- corruption prevention resources that are being used or would be useful to other state government agencies.

IBAC also published research on employee perceptions of corruption in 2017. Surveys were conducted with state government, local government and Victoria Police employees, as well as members of the Victorian community.[11]

Where relevant, this report refers to the 2017 research, and discusses differences observed between the 2014 and 2019 reviews.[12]

2.1.2 Regulatory requirements and policy guidance

In Victoria, departments and relevant public entities are required to meet certain legislative responsibilities that are relevant to their integrity frameworks. These include:

- *Public Administration Act 2004*, which sets out public sector values and employment principles to guide public sector employees and agencies.
- *Financial Management Act 1994* and associated Standing Directions of the Minister for Finance which require relevant agencies to take all reasonable steps to manage fraud and corruption risks, develop a policy to govern the management and prevention of fraud, corruption and other losses, audit business processes that are likely to be vulnerable to corruption, and report incidents of significant or systemic fraud and corruption.
- *Independent Broad-based Anti-corruption Commission Act 2011* (IBAC Act), which mandates relevant principal officers of public sector agencies must notify IBAC of suspected corrupt conduct, and the *Protected Disclosure Act 2012* (PD Act) which sets out procedural requirements to facilitate reports, and provides protections for people who make disclosures.
- Code of Conduct for Victorian Public Sector Employees, which is binding for all VPS employees and prescribes standards of required behaviour.

The Victorian Public Sector Commission (VPSC) is responsible for issuing the Code of Conduct and plays a central role in promoting ethical conduct in the public sector, developing and promoting tools and resources to build awareness and understanding of integrity. This includes a model Conflict of Interest Policy and a Gifts, Benefits and Hospitality Policy Framework.

[10] IBAC 2014, *A review of integrity frameworks in Victorian public sector agencies*, Melbourne.

[11] IBAC 2017, *Perceptions of corruption, Survey of Victorian state government employees*, Melbourne.

[12] Where questions allowed for comparison of results and responses.

The Victorian Government Purchasing Board (VGPB) plays a key role in promoting good practice in procurement in state government. Key guidance includes the Procurement Framework and Supplier Code of Conduct, which has applied to suppliers since 1 July 2017, in part to address issues identified in IBAC's 2016 *Perceptions of corruption: Survey of Victorian Government suppliers*.

The Office of the Victorian Information Commissioner has developed a Victorian Protective Data Security Framework, which sets out 18 high-level mandatory requirements in the governance and protection of public sector data.

The Department of Health and Human Services has developed an Integrity Governance Framework and Assessment Tool for Victorian public health services. The purpose of the framework and tool is to help health services assess their integrity risks and to provide guidance on the development of policies and procedures to reduce the risk of fraud and corruption.[13]

IBAC has also published special reports on a number of investigations, research reports, case studies and other resources that highlight possible corruption risks and opportunities to strengthen practices and controls. Those matters have repeatedly highlighted corruption risks pertaining to:

- procurement practices
- conflict of interest
- employment practices
- information management
- monitoring and supervision
- organisational culture.

2.2 Methodology

2.2.1 Organisational integrity framework survey

IBAC invited 50 Victorian state government agencies to participate in the review, representing a broad range of agencies across the spectrum of public sector services and functions, ranging from small, specialised regulatory and statutory authorities to the seven major departments.[14]

The organisational integrity framework survey was conducted between December 2017 and February 2018, and responses were received from 38 of the 50 agencies invited to participate (76 per cent).

The survey comprised 51 questions, broadly categorised as follows:

- key policy documents in place to govern integrity and guard against fraud and corruption
- perceptions of the extent to which a number of potential corruption risks were considered a risk to the agency
- information and education to support integrity, fraud and corruption awareness initiatives
- internal reporting mechanisms in place, including protected disclosure mechanisms
- ways in which suspected corrupt conduct has been identified (where relevant)
- ways in which corruption prevention and integrity measures are promoted and reinforced
- other integrity initiatives implemented by agencies.

Agencies were advised that for the purposes of this review, corruption excluded misconduct such as assault, sexual harassment, bullying or poor performance. It included criminal offences such as theft or fraud if those offences involved the misuse of information or material acquired in the course of the performance of a role or function.

[13] health.vic.gov.au/about/publications/policiesandguidelines/Integrity-governance-framework-and-assessment-tool-resources

[14] At the time the review was conducted, there were seven departments.

Agencies were asked to identify and provide the primary policy documents that govern integrity and guard against fraud and corruption within their organisations. IBAC's aim was to gauge the types of policies agencies considered most relevant to their integrity frameworks and identify if there were initiatives other agencies could consider. As such, while codes of conduct and conflict of interest policies were provided as examples of the types of policies agencies might consider, the survey did not prescribe key policies to be provided.

More than 500 policies, procedures and other resources were provided and reviewed. Most of the agencies provided documentation relating to:

- fraud and corruption control
- codes of conduct
- conflict of interest
- gifts, benefits and hospitality
- supplier engagement
- protected disclosures.

These key policy documents and agencies' responses to the survey were broadly assessed against the Australian Standard AS 8001-2008 Fraud and Corruption Control.

Survey limitations

This review did not involve a comprehensive audit of relevant policies. Rather, agencies were invited to provide what they considered to be the main policy documents relevant to their integrity frameworks. As such, the documentation provided did not always address all key elements of the Standard. However, IBAC understands those elements could be covered in other agency policies.

Many questions in the survey were open-ended to explore initiatives agencies have implemented. The questions did not always align with the 2014 review or the 2017 survey of state government employees. As a result, direct comparison was not always possible.

2.2.2 Consultation

Following analysis of the survey responses, 10 agencies were selected for consultation to explore their responses in greater detail, as well as the corruption prevention resources and initiatives those agencies have in place, the challenges they face, and opportunities for improvement.

The agencies involved in these consultations were selected because they broadly represented the three tiers used in this review and the results of the survey analysis.

Consultations were conducted in May 2018 and included three agencies from Tier 1, four from Tier 2 and three from Tier 3.

Consultation limitations

Agencies nominated their representatives for the consultations. Due to time constraints and the experience and knowledge of the agency attendees, topics discussed and the depth of the discussions varied. Direct comparison between agencies' experiences was not always possible.

3 Risk management

This section looks at fraud and corruption control frameworks in terms of planning and risk assessment, before considering policies and practices described by agencies to manage specified fraud and corruption risks.

3.1 Fraud and corruption control frameworks

3.1.1 Fraud and corruption control planning

Guidance in the Standard suggests organisations should develop and implement a fraud and corruption control plan that documents their approach at strategic, tactical and operational levels. The plan should detail the entity's intended actions in implementing and monitoring fraud and corruption prevention, detection and response initiatives. According to the Standard, organisations are advised to:

- Develop the plan, accounting for existing policies dealing with fraud and corruption risk, and avoid duplication, inconsistency and uncertainty. The plan should be viewed as a comprehensive framework for addressing fraud and corruption risks.
- Monitor the plan's operation by setting out internal and external processes, key milestones and objectives. The resources and objectives should be appropriate for the organisation's current operations.
- Communicate the plan to all staff and external stakeholders, for example through declarations in requests for tender or supplier invitations, and on the organisation's intranet and website.
- Review the plan at appropriate intervals, but at least every two years. Factors to consider when reviewing the plan include changes to the organisation's fraud and corruption control objectives, significant changes in the operating environment, strategies arising out of recently detected incidents, results of risk assessments, resourcing requirements, and changes in fraud and corruption control practices locally and internationally.

A plan can help to consolidate relevant fraud and corruption control resources, ensure a consistent approach across the organisation and identify whether further work and additional resources are required. As the Western Australian Corruption and Crime Commission has noted:

> *'Simply introducing more controls, policies and systems is not enough to build a misconduct-resistant public body. In fact, without careful planning, they can produce administrative inefficiency and reduce performance.'*[15]

Agencies should view their fraud and corruption control plan as a mechanism to guide the development and coordination of other fraud and corruption control activities.

3.1.1.1 Policies

Most agencies across all three tiers provided evidence of a fraud and corruption control plan. The documentation provided included statements that suggested plans were regularly reviewed and amended at two to three-year intervals, and upon becoming aware of significant change in the operating environment. The content of those documents also suggested agencies across all tiers were generally aware of the importance of developing a plan, and considered it a key part of their corruption risk management.

Only two agencies did not provide fraud and corruption plans or other similar documentation as part of this review. A third agency that did not have a fraud and corruption plan provided a fraud training and awareness plan that listed activities proposed or undertaken in the previous 18 months.

As discussed in the case study on the following page, developing a fraud and corruption plan is only the start. Responsibilities allocated under a plan must be clearly communicated to relevant employees and reiterated more broadly across the organisation to be effective.

[15] Western Australian Corruption and Crime Commission 2008, *Misconduct Resistance*, Perth, p.2.

CHALLENGES INVOLVED IN IMPLEMENTING A FRAUD AND CORRUPTION CONTROL PLAN

Case study 1

In creating its Fraud and Corruption Control Policy and Plan, one Tier 2 agency noted it engaged its leadership and audit teams to create appropriate risk compliance guidelines and procedures. The agency engaged a legal firm to develop a legislative compliance checklist relevant to its operations. Internal committees assessed the organisation's success in responding to integrity compliance measures by following the legal checklist. In future, the agency intends to conduct an annual risk assessment to consider its fraud and corruption risks and implement appropriate controls.

The agency's Fraud and Corruption Control Policy and Plan was created in January 2018 and is being distributed and implemented. It may take some time for the plan to be embedded in the organisation. For example, in consultations it became evident certain units were not yet aware of specific fraud and corruption control responsibilities allocated to them under the plan. The agency subsequently advised confusion may have arisen over a comment made during consultations regarding a decision to transfer responsibility for the agency's fraud and corruption guideline from one work unit to another. However, the agency is confident all employees with responsibilities under the policy have a clear understanding of their duties.

3.1.1.2 Practices

In open-ended responses, some agencies referred to their plans as a control tool as well as providing an opportunity to communicate with staff when the plan was updated. For instance, one agency referred to its plan when describing controls to prevent bribery risks. Another agency noted its policies and plans were regularly reviewed, and any changes discussed at leadership meetings and communicated more broadly to affected staff.

Consultations confirmed agencies across all tiers considered their fraud and corruption control plan to be a key element in promoting integrity throughout their organisations. Some organisations said they conducted a preliminary assessment of fraud and corruption risk before developing their plan, by engaging internal or external audit providers and subject matter experts. Other planning initiatives included the appointment of a fraud and corruption control officer, and convening an integrity forum comprising representatives from across the organisation responsible for managing the plan and the agency's exposure to corruption risks.

3.1.2 Fraud and corruption risk assessment

Guidance in the Standard suggests organisations should adopt a policy and process for the systematic identification, analysis and evaluation of fraud and corruption risks, and periodically conduct a comprehensive assessment of those risks within their organisations.

It is good practice for fraud and corruption risk assessments to be conducted in accordance with the Australian and New Zealand Standard, *Risk Management Principles and Guidelines* (ANZS 4360:2004) which outlines a seven-stage risk management principles approach including:

- communicating and consulting to understand the agency's operations and functions
- establishing the context including the internal, external and risk management environments
- identifying risks by considering what could happen, when and where it would happen, and how and why it would happen
- analysing risks by identifying the controls and determining risk levels after considering consequences and likelihood of the risks
- evaluating risks by prioritising them
- treating risks by identifying and assessing options, preparing and implementing treatment plans, and analysing residual risk levels to determine whether they are tolerable
- monitoring and reviewing whether implemented controls are effective in treating the risks identified and if any new, emerging risks need to be evaluated and treated.

Agencies should take into account their size, function, any external or internal changes, and their specific risk appetite when conducting fraud and corruption risk assessments.

Risk assessment programs should be conducted at each operational unit level, documented, reviewed and updated periodically to ensure new and emerging fraud and corruption risks are identified, and the efficacy of any controls that have been implemented are assessed.

A key finding in the 2014 review was although most participating agencies reported having risk assessment processes related to financial, audit or fraud risks, very few reported having specific corruption risk assessments.

The current review prompted agencies to reflect on the extent to which specific issues were considered a corruption risk for the agency and to indicate whether that risk was recorded and managed as discussed in section 3.2.

Responses suggest conflict of interest, improper procurement, and improper cash handling or payment arrangements were the issues most frequently controlled for and recorded on risk registers, which may suggest financial and fraud-related corruption risks continue to be the focus of agencies.

3.1.2.1 Policies

The documentation provided indicated agencies across all tiers had defined corruption in their framework, however consideration of external risk scenarios (such as cyber-attacks that could compromise personally identifiable information) was generally not demonstrated.

Consultation with selected agencies suggested fraud and corruption risk assessments were carried out periodically, although the level of detail relating to the conduct and frequency of these risk assessments varied. While the documentation provided by agencies did not always address the assessment, monitoring and review processes used by agencies to identify corruption risks and controls, the policies provided suggest some agencies may have documented those processes separately.

3.1.2.2 Practices

The survey listed specific corruption risks and asked agencies to indicate whether each one was considered a risk to the organisation, recorded on the agency's risk register, and mitigated through controls (see section 3.2). Several agencies referred to their risk assessment processes in discussing the types of controls they had in place to manage corruption risks. Those processes ranged from targeted assessments for particular corruption risks to corruption risk assessments that explore and address risks and controls at all levels of the organisation. For example:

- One Tier 2 agency described an organisation-wide corruption risk assessment process in relation to high-risk areas of the business that takes place annually at a minimum. The process involves a 'system of internal controls that are documented and updated for activities and processes that are assessed as posing a higher risk'.
- Another Tier 2 agency noted it has an operational guideline to ensure good practice in procurement, against which the procurement team is required to assess probity risks.

In general, the corruption risk assessment processes described by agencies aligned with the maturity of their integrity framework. Agencies that had more developed integrity frameworks were more aware of and attuned to the types of corruption risks their agency may face, regardless of the size of the agency, as demonstrated in the following case studies.

CORRUPTION RISK ASSESSMENT PROCESSES THAT ARE FIT FOR PURPOSE

Case study 2

In one Tier 1 agency, an internal audit team conducts risk assessments specifically relating to fraud and corruption. Individual risks are rated on a scale of low, medium and high, then assessed according to the business group to which they relate. Retail and procurement are key operational areas the internal audit team assesses for fraud and corruption risk. For example, cash handling risks have been assessed in relation to the agency's retail function. Procurement risks are assessed before engaging suppliers and service providers. The agency's corporate governance team is guided by internal audit risk assessment results and maintains a risk register. In consultations, the agency advised it is building an assurance program that will formalise the organisation's risk assessment procedures, and the roles and responsibilities of the risk management business unit.

Case study 3

One Tier 3 agency advised it has dedicated significant resources to corruption risk management, governance and audit. The department's risk leadership conducts regular integrity workshops to develop and monitor the agency's official integrity framework and integrity improvement program. The department actively records and monitors program risks and strategic risks, and divisional risk registers are maintained. Integrity and corruption are a specific risk category on the register. The risk register is also integrated into the business planning and performance monitoring system, which is assessed monthly. Internal audit conducts regular reviews of the risk registers, and business units use a panel to undertake assurance work and recommend controls to mitigate risks.

3.2 Assessment of specific risks

Agencies were asked to indicate the extent to which listed issues were considered a corruption risk, whether the issue was recorded on the agency's risk register, and if the agency had any controls in place to manage each risk. Agencies were then asked to comment on the reasons for the risk rating (where relevant), and any controls in place within the agency to manage the risk. The potential corruption risks were:

- improper procurement arrangements
- hiring one's own company or the company belonging to a friend or family to provide public services
- improper cash handling and/or payment arrangements
- misuse of information or material
- conflict of interest
- hiring friends or family for a government job
- abuse of discretion
- improper funding arrangements and/or use of grants
- bribery.

Agencies were also asked to list any other corruption risks identified by their organisations. Those responses are discussed in section 3.2.10.

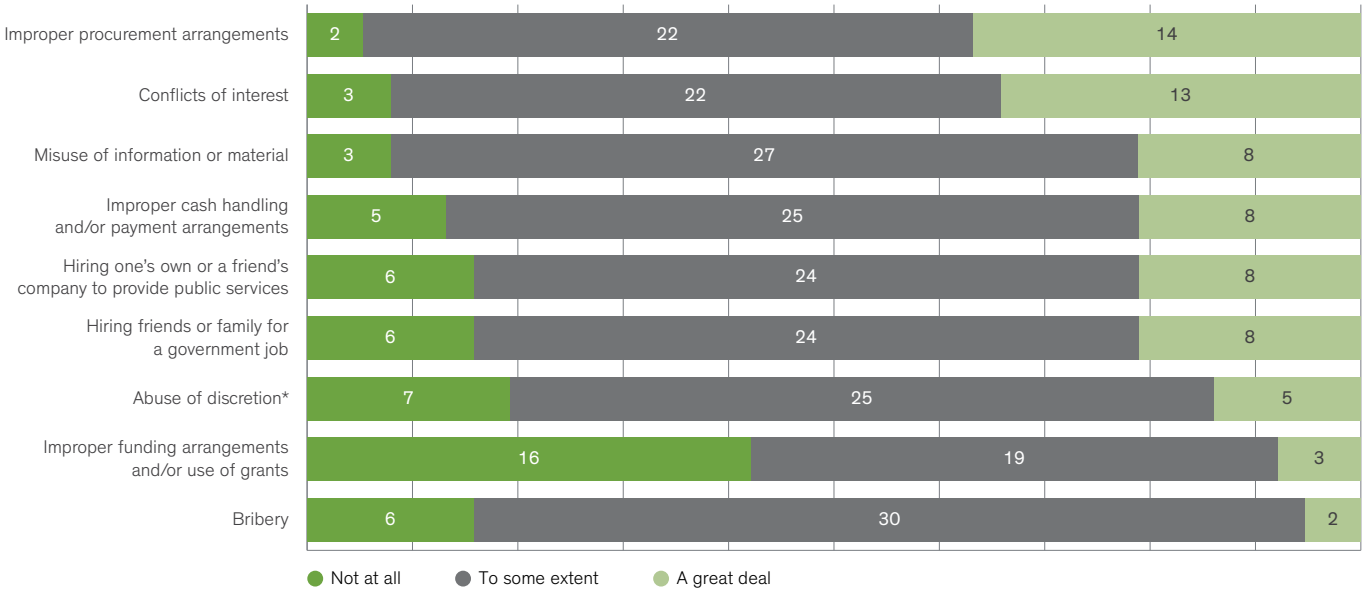
Perceived exposure to corruption risks

Most agencies demonstrated a clear understanding of the specific corruption risks listed in the survey, compared to the 2014 review which identified 'corruption is generally not on the radar of the responding agencies'. However in consultations, when specific risks faced by agencies were discussed, it was evident some agencies had a limited view of corruption risks.

As shown in Figure 1, of the nine risks, improper procurement was considered to pose a corruption risk by the largest proportion of participating agencies (36 agencies), followed closely by conflict of interest and misuse of information or material (35 each). This is broadly consistent with the 2014 review, in which procurement was the most commonly reported risk nominated by respondent agencies.[16]

[16] IBAC 2014, *A review of integrity frameworks in Victorian public sector agencies*, Melbourne, p 5. The most commonly reported risks and their most common classifications were: procurement (medium or high risk), breach of IT or information security (medium or high risk), and financial misconduct by employees (high, medium and low risk).

FIGURE 1. EXTENT TO WHICH IDENTIFIED ISSUES WERE CONSIDERED TO BE A CORRUPTION RISK



n = 38 agencies
** 'Abuse of discretion' does not total 38 because one agency did not provide a response to this question.*

These results are consistent with the findings of the 2017 survey of Victorian state government employees. In that survey, respondents most commonly stated there were opportunities for conflict of interest in their agency, followed by misuse of information or material, and hiring friends or family for public service jobs.[17]

Both the current review and 2017 survey of state government employees indicate there is a growing recognition of the need to consider a broader range of corruption risks, such as conflict of interest. Conflicts of interest can arise in key operational areas such as procurement, recruitment and certification/qualification review processes, and can facilitate corrupt conduct if not properly managed.

Identification of corruption risks in risk registers

With the exception of cash handling and procurement arrangements,[18] it was apparent there was sometimes a disconnect between an agency acknowledging its exposure to a risk and that risk being recorded on the agency's risk register to ensure the risk is controlled and monitored. In particular:

- Of the 32 agencies that stated hiring friends or family for a government job posed a corruption risk to the agency, 11 stated the issue was not on their risk register.
- Of the 32 agencies that stated bribery posed a corruption risk to the agency, eight stated the issue was not on their risk register.
- Of the 22 agencies that stated improper funding arrangements and/or use of grants posed a corruption risk to the agency, six stated the issue was not on their risk register.

[17] IBAC 2017, *Perceptions of corruption: Survey of Victorian state government employees*, Melbourne, p.8: 62 per cent of respondents said there were opportunities for conflict of interest to occur in their agency, 56 per cent said misuse of information and 51 per cent said hiring friends or family for public service jobs.

[18] Four of the 33 respondent agencies that stated improper cash handling poses a corruption risk to the agency (a risk to 'some extent' or 'a great deal') also stated the issue is not on the organisation's risk register, while five of 36 respondents that stated improper procurement arrangements pose a corruption risk to the agency also stated the issue is not on the organisation's risk register.

Application of relevant controls to mitigate corruption risks

Most agencies indicated controls were partly or comprehensively in place to manage the relevant risk. The controls noted by agencies generally fell into the following categories:

- policies and procedures[19]
- training and communication[20]
- data analytics[21]
- audits[22]
- reporting[23]
- declarations[24]
- employee screening and recruitment processes[25]
- supplier due diligence[26]
- delegations of authority.[27]

A number of agencies also stated they had comprehensive controls in place to manage certain corruption risks, however the controls described did not appear to be sufficient to fully mitigate the risks. For example, the controls described by agencies were sometimes limited to policies and procedures such as their fraud and corruption policy and plan, code of conduct and other integrity policies.

While policies are an important element of an agency's integrity framework, they should be complemented and supported by operational controls to detect and mitigate fraud and corruption risks, as well as initiatives to promote ethical culture and leadership more generally.

3.2.1 Improper procurement arrangements

Perceived risk

Fourteen agencies stated improper procurement arrangements pose a great risk to their organisation. Twenty-two agencies stated this risk was relevant to their organisation to some extent, while two agencies stated this was not a risk to their organisation at all.

The two agencies that did not consider improper procurement arrangements to pose a risk to their organisation said that comprehensive controls were in place to effectively manage this risk in their organisation. Specifically:

- One Tier 1 agency noted controls in place to manage the risk included policies, templates and procurement practices, compliance with VGPB requirements, and financial monitoring mechanisms.
- One Tier 2 agency noted the risk was comprehensively recorded on its risk register, adding comprehensive staff induction, and ongoing awareness programs and communications ensured employees were aware of this risk.

Of the 36 agencies that considered improper procurement arrangements were a risk to their organisation, five indicated the risk was not recorded in their risk registers. However, all five indicated that controls were partly or comprehensively in place to manage this risk.

[19] See section 4.1.1.1 for further discussion of policies and procedures.
[20] See section 4.2 for further discussion of training and communication.
[21] See section 5.1 for further discussion of data analytics.
[22] See section 5.3 for further discussion of audits.
[23] See section 5.2 for further discussion of reporting channels.
[24] See section 4.1.2.2 for further discussion of declaration processes.
[25] See section 3.2.6 for further discussion of employment screening and recruitment processes.
[26] See section 3.2.1 for further discussion of supplier due diligence.
[27] See section 3.2.7 for further discussion of delegations of authority.

Controls

Irrespective of whether agencies considered improper procurement arrangements to be a corruption risk to their organisations, all 38 said their organisation had controls partly or comprehensively in place to manage the risk. Twenty-seven described specific controls including:

- Policies and procedures: the organisation's procurement framework, policies and guidelines relating to conflict of interest, code of conduct, contract management, financial management, outsourcing, delegations, probity, protected disclosures, and fraud, corruption and other losses prevention.[28]
- Segregation of duties: measures designed to improve the independence of procurement processes such as engagement of an external probity advisor for large-scale procurement, establishment of an independent, internal procurement unit or role that centrally oversights high value procurement activities, and appointment of a dedicated procurement board (with an independent chair) with responsibility for endorsing high-value procurement strategies, initiating audits to check for compliance with purchasing policies and procedures, and reviewing audit reports as well as providing an escalation point in the procurement complaints management process.[29]
- Delegation of authority/multi-level approvals: requiring approval at a number of levels at key points in the procurement process (eg selection of the panel, contracting and variation in contracts) in accordance with approved delegations of authority.[30]
- Conflict of interest declarations: specifically for procurement panel members and others involved in procurement, which some agencies embed in procurement checklist processes.[31]
- Training and communication: such as training, ongoing awareness-raising programs and communication on relevant policies and procedures, procurement and contract management systems, and financial delegations.[32]
- VGPB requirements: noting suppliers and contractors are required to comply with the Victorian Government Supplier Code of Conduct.[33]
- Audit activities: in relation to procurement and conflicts of interest.[34]
- Management oversight: for example, one agency noted its board has oversight of procurement valued at more than $2 million, while another noted it has a dedicated procurement unit that oversights all procurement activities.[35]
- Internal reconciliation and review: through financial tracking and monthly financial reporting.[36]
- System controls: such as processes to support the agency's policy requirements to conduct assessments of probity risk, complexity and capabilities.[37]
- Due diligence: such as conducting referee checks of prospective suppliers.[38]

[28] 23 agencies.
[29] Ten agencies.
[30] Seven agencies.
[31] Five agencies from Tiers 1 and 2.
[32] Five agencies from Tiers 2 and 3.
[33] Five agencies from Tiers 1 and 3.
[34] Three agencies.
[35] Two Tier 2 agencies.
[36] Two agencies from Tiers 1 and 2.
[37] One Tier 2 agency.
[38] One Tier 2 agency.

PROCUREMENT CONTROLS

Case study 4

At one Tier 2 agency, suppliers with the largest procurement value are reported to the risk and audit committee, while the board has oversight of all procurement procedures. Financial management controls are enforced through creditor reviews, and accounts payable/payment file audits. The agency uses labour agencies from a panel of suppliers to assist with staffing shortfalls. During consultations, the agency noted it does not perform due diligence on these suppliers because due diligence has already been conducted through the panel arrangement.

As noted in the NSW ICAC's 2018 report, *Corruption and integrity in the NSW Public Sector*, 'agencies should not assume all empanelled suppliers have been subjected to an exhaustive set of due diligence checks'.[39] It is good practice for agencies to conduct their own checks.

In response to the question about improper procurement arrangements, only one agency said it conducted any form of due diligence before engaging a supplier. However, six agencies discussed conducting due diligence as a control for the risk of hiring one's own company or the company belonging to a friend or family member to provide public (for example by cross-checking supplier information against employee information to identify potential conflicts of interest) more widely than reported in responses to the survey.

Due diligence of prospective suppliers in the form of background checks, supported by declarations by the supplier, can greatly assist an agency to fully understand the risks associated with doing business with that supplier, including potential conflict of interest risks in procurement. The level of due diligence required will depend on the risks associated with each supplier. The assessment should take into account a range of factors including the anticipated value of the procurement, the nature of the goods or services to be provided, whether there are any industry-specific risks, and the financial profile and reputation of the supplier.

Due diligence should involve validating information collected from the supplier and independent sources, where possible, to determine whether the potential suppliers with individuals associated with the supplier pose any unacceptable risks. It is also good practice to compare supplier details against employee declarations to identify any risks or potential conflicts of interest that may not have been declared.

The due diligence process should be conducted periodically to ensure changes in a supplier's circumstances do not pose increased risks to an agency.

[39] NSW Independent Commission Against Corruption 2018, *Corruption and integrity in the NSW public sector*, Sydney, p.55.

3.2.2 Hiring one's own company or the company of a friend or family member

Perceived risk

The risk of hiring one's own company or the company of a friend or family member was canvassed in the survey to gauge agencies' perceptions and controls in place to manage this risk. This risk is a sub-set of improper procurement and should be controlled through robust procurement processes.

Eight agencies stated hiring one's own company or the company belonging to a friend or family member to provide public services posed a great risk to their organisation. A further 24 agencies stated this risk was relevant to their organisation to some extent, while six agencies stated it was not a risk to their organisation at all.

Five of the six agencies that did not consider hiring one's own company or the company belonging to a friend or family member to be a corruption risk to their organisation, noted controls were partly or comprehensively in place to manage this risk. This may indicate they consider their controls have effectively negated the residual risk of hiring one's own company or the company of a friend or family member. One of these five agencies also advised the services it procures are very limited because it is a comparatively small administrative office, reducing its exposure to this risk.

Of the 32 agencies that consider hiring one's own company or the company belonging to a friend or family member to pose a risk to their organisation, seven indicated the risk was not recorded in their risk registers. However, all seven indicated controls were partly or comprehensively in place to manage this risk.[40]

Controls

Thirty-six agencies advised their organisations had controls partly or comprehensively in place to manage the risk of hiring one's own company or the company of a friend or family member. Thirty agencies commented on the specific controls in place, most of which were the same as the controls identified to manage the risk of improper procurement arrangements, with an added focus on managing conflicts of interest in procurement.

For example, six agencies said they conduct supplier due diligence for all new suppliers or suppliers beyond certain procurement value thresholds.[41] However, one Tier 2 agency noted while it checks supplier information against Australian Securities and Investments Commission registers, it recognises the information obtained is of limited assistance in detecting risks or concerns with suppliers. Similarly, a Tier 3 agency noted that while it had made improvements to due diligence performed on suppliers and cross-checks details against declarations of private interests, it recognises this risk still exists.

Ten agencies require employees to disclose conflicts of interest, particularly those assigned to a tender selection panel.

[40] One further Tier 3 agency that considered this issue a risk 'to some extent' did not respond to questions regarding controls or recording of the issue in its risk register.

[41] The six included agencies from all three Tiers.

3.2.3 Improper cash handling and/or payment arrangements

Perceived risk

Eight agencies stated improper cash handling and/or payment arrangements posed a great risk to their organisation. A further 25 agencies stated this risk was relevant to their organisation to some extent, while five agencies did not consider this a risk to their organisation at all.

Several agencies that considered this risk relevant to their organisation noted their activities require cash payments from the public. For example, one Tier 2 agency noted 'community members accessing services regularly undertake cash or payment transactions with employees', while another commented the organisation has a 'high volume of cash handling and/or payment arrangements'.

All five agencies that did not consider improper cash handling and/or payment arrangements a corruption risk to their organisations said that controls were partly or comprehensively in place to manage this risk. This may indicate these agencies consider their controls have sufficiently mitigated the level of residual risk. For example, one Tier 2 agency that handles cash said it takes a serious approach to this risk and had minimised its exposure by applying a range of relevant controls including cash-handling procedures (eg daily reconciliation, sign-off processes and requirements to transfer cash into a 'cash room' at regular intervals) and regular reviews of its cash-handling processes through its internal audit program.

Of the 33 agencies that considered improper cash handling and/or payment arrangements to pose a risk to their organisation, four indicated the risk was not recorded in their risk registers. However, all four agencies indicated controls were partly or comprehensively in place to manage this risk.[42]

Controls

Irrespective of whether agencies considered improper cash handling and/or payment arrangements to be a corruption risk to their organisations, 37 agencies advised their organisation has controls partly or comprehensively in place to manage the risk. Twenty-one agencies described specific controls including:

- Policies and procedures: such as those governing financial management, petty cash, cash management, procure-to-pay procedures, purchasing, credit card and purchase card use.[43]
- Audit activities: such as internal and/or external audit and review activities.[44] For example, one agency noted 'recent internal audit responses have led to broad reform and removal of many cash handling functions'.
- Segregation of duties: for example, one agency said that receivable and banking duties are separated.[45]
- Internal reconciliation and review: such as cash transaction reconciliations, frequent monitoring, and review and reconciliation mechanisms.[46]
- Training and communication: in relation to cash handling and financial management for staff responsible for the processes.[47]
- Delegation of authority/multi-level approvals: such as multi-level approval for cash transactions.[48]
- System controls: such as an electronic procure-to-pay system to limit the need for employee cash expenses.[49]

The case studies on the following page illustrate how approaches to controlling risks associated with improper payment arrangements should be tailored to the risk profile and needs of an organisation.

[42] One further Tier 3 agency that considered this issue a risk 'to some extent' did not respond to questions regarding controls or recording of the issue in its risk register.

[43] 13 agencies.

[44] Nine agencies.

[45] Seven agencies.

[46] Six agencies from Tiers 1 and 2.

[47] Five agencies from Tiers 1 and 2.

[48] Four agencies.

[49] One Tier 1 agency.

PAYMENT CARD CONTROLS

Case study 5

A Tier 3 agency advised it has 350 corporate card cards in use, and a range of controls in place to manage the use of those cards, including:

- All staff receive training on credit card usage.
- Expenses are reviewed by the employee's manager monthly.
- Each employee's credit card transactions are audited at least once a year.
- Three staff work on compliance reviews and conduct monthly reconciliations of corporate credit cards. Data analytics is used in this process and has often detected policy breaches.
- The finance team also checks transactions related to accommodation, flowers, restaurants, and duplicate payments – especially transactions incurred at weekends.

Case study 6

A Tier 1 agency advised it only has two corporate credit cards in use to minimise their risk exposure. These cards are only used by the Finance Manager and the Chief Operating Officer. In addition, reports are run regularly on approved transactions to ensure compliance with policy.

3.2.4 Misuse of information or material

Perceived risk

Eight agencies stated misuse of information or material poses a great risk to their organisation. A further 27 agencies stated this risk is relevant to their organisation to some extent, while three agencies said it is not a risk to their organisation at all.

The eight agencies that considered misuse of information or material a great risk provided a number of reasons for their rating including reputational damage and breach of privacy or other legislation, compromising the (regulatory), nature of the agency's work given the amount of confidential third party information held by the agency, and the fact that the agency holds 'large quantities of sensitive and valuable information'.

The three agencies that did not consider misuse of information or material a risk to their organisation included one agency that noted the risk was partly recorded on their risk register and comprehensive controls were in place to manage the risk. This may indicate the agency considered the residual risk to be negligible given the controls in place.

Of the 35 agencies that considered misuse of information or material poses a risk to their organisation, six indicated the risk was not recorded in their risk registers. However all six also indicated controls were at least partly in place in their organisations to manage this risk.[50]

In consultations, one agency that considered misuse of information or material to be a risk to the organisation advised it had experienced numerous 'phishing' attacks which prompted the introduction of controls. This agency noted the specific issue of 'misuse of information' was not recorded in its register, but subsequently advised three risks on the register related to the confidentiality and security of personal and other information.

[50] One further Tier 3 agency that considered this issue a risk 'to some extent' did not respond to questions regarding controls or recording of the issue in its risk register.

Controls

Irrespective of whether agencies considered misuse of information or material to be a corruption risk to their organisations, 35 agencies advised their organisation had controls partly or comprehensively in place to manage the risk. Twenty-two described specific controls including:

- Policies and procedures: such as codes of conduct and policies concerning data security, privacy and data protection, data classification, IT usage, financial management and clean desk requirements.[51]
- System controls: such as access controls, password and user name protections, and processes to maintain audit trails.[52]
- Training and communication: for example, induction, ongoing awareness programs and communication to staff in relation to asset management, confidentiality and privacy.[53]
- Audit activities: such as internal and external audit and review activities on data security control systems and record-keeping protocols.[54]
- Internal reconciliation and review: such as monitoring systems to identify potential data theft, suspicious system activities and network intrusions.[55]
- Third party confirmation: through confidentiality clauses in third party contracts and privacy agreements.[56]

Segregation of duties was also identified as a relevant control without detailing how it specifically helped the agency mitigate the risk of information or material misuse.[57]

Compared with the 2014 review, in which breach of IT or information security was considered a significant risk by the agencies, this review suggests systematic controls have been established and implemented by agencies to enhance their information technology and information security capacity. This may be due, in part, to the introduction of the Victorian Protective Data Security Standards, introduced in July 2016, as discussed in the case study on the following page.

[51] 18 agencies from all three tiers.
[52] Nine agencies from all three tiers.
[53] Six agencies from Tiers 2 and 3.
[54] Four agencies from Tiers 1 and 2.
[55] Two Tier 2 agencies.
[56] One Tier 2 agency.
[57] One Tier 1 agency.

INFORMATION TECHNOLOGY CONTROLS

Case study 7

One Tier 2 agency noted it had implemented a range of information security controls. The organisation uses an information security management framework, which contains policies and procedures related to use of technology systems.

Examples of IT controls included 90-day password resets, naming of user accounts, separation of duties, and data analytics. Emails are monitored, logged and archived, and staff receive annual information security refresher training. Security penetration testing is also conducted annually by external parties. Higher levels of access are monitored and provided to employees only with a relevant work requirement.

The agency also has an information security officer dedicated to enforcing and controlling integrity in IT. And it utilises data analytics in the form of a security information management system which monitors the entire network and identifies unusual behaviour. For example, if an employee downloads or copies a large file, this is flagged and followed up via a phone call and physical inspection.

Case study 8

One Tier 3 agency noted that due to the sensitive nature of the data it maintains, it has a number of measures in place (in addition to CenITex data security controls) to control misuse of information. The department advised these controls have been reviewed and strengthened, consistent with Victorian Protective Data Security Standards. They include:

- maintaining audit trails for log-ins
- access controls to sensitive documents
- separate, secure cabinets for confidential material
- access controls for after-hours access to the building
- frequent communication of clear-desk policy requirements
- encrypted USB requirements for document transfers
- secure printing arrangements requiring the use of a passcode to collect confidential documents and removal of documents from the queue, if documents are not collected within a certain time
- lock-screen security and laptop shutdown if inactive for two hours.

To make employees aware of the IT security requirements, the department recently rolled out communication on its intranet detailing good information security behaviours. It also intends to run a competition related to good information security behaviour, to encourage staff to participate in the campaign.

A number of agencies noted ongoing efforts to develop frameworks and/or technology capability to further control the risk of misuse of information. For example, one Tier 3 agency noted 'use of information for private gain is a significant risk… [and] strengthened information management policies and procedures are being developed', while a Tier 2 agency said it was working on developing a protective data framework.

3.2.5 Conflict of interest

Perceived risk

Thirteen agencies stated conflicts of interest posed a great risk to their organisation. A further 22 agencies said this risk was relevant to their organisation to some extent, while three agencies stated they did not consider it a risk to their organisation at all. Each of these three advised that comprehensive controls were in place to manage the risk. It is possible these agencies have therefore assessed the residual risk as negligible. For instance, one agency noted it 'takes conflicts of interest seriously' and had 'implemented policy and practices to ensure disclosure requirements are rigorous across the organisation' including in procurement, employment and other areas in which personal interests could be perceived to affect how staff carry out their duties.

In consultations, another agency clarified its survey response noting it considered conflict of interest as a significant risk and had controls in place, including staff induction, and ongoing awareness programs and communication to promote employee awareness of this risk.

Most agencies consulted had conflict of interest procedures in place. Some maintain conflicts declared by employees electronically and others maintain the declarations in paper form.

Of the 35 agencies that considered conflicts of interest posed a risk to their organisation, six indicated the risk was not recorded in their risk registers. However, all of these agencies indicated controls were partly or comprehensively in place to manage this risk.

Controls

Irrespective of whether agencies considered conflict of interest to be a corruption risk to their organisations, all 38 agencies advised their organisation had controls partly or comprehensively in place to manage the risk. Twenty-five described specific controls including:

- Policies and procedures: such as conflict of interest policies, guidelines and procedures, disclosure of interest guidelines, human resources recruitment and selection checklists, management approval policies, codes of conduct, procurement-related policies and guidelines, secondary employment policies as well as gift, benefit, and hospitality policies.[58]
- Declaration processes: in relation to conflicts of interest, private interest and gifts, benefits and hospitality as well as registering those details in a way that enables cross-checking. Processes included requiring declarations upon employment with the agency, and at key stages in particular activities such as decisions on major projects, procurement, recruitment and regulatory inspections.[59]
- Training and communication: for example, one agency noted all staff undergo training on conflict of interest during induction and annual refresher training.[60]
- Management oversight: for instance, through the inclusion of 'conflict of interest' as a standing agenda item for relevant committees.[61]
- Internal reconciliation and review: such as the development and implementation of data analytic capabilities to identify potential conflicts.[62]
- Delegation of authority/multi-level approvals: such as financial delegation requirements.[63]

[58] 19 agencies from all three tiers.

[59] 14 agencies from all three tiers.

[60] Five agencies from all three tiers.

[61] Four agencies from Tiers 1 and 2.

[62] Two agencies from Tiers 1 and 3.

[63] Two agencies from Tiers 1 and 2.

In consultations, one Tier 3 agency noted it recorded conflict of interest and private interests in paper form, which was later entered into spreadsheets that were not managed centrally. Recognising the limitations of this approach, the agency is looking to develop an electronic process to capture details of declared conflicts of interest and private interests with a view to utilising data analytics.

The following case study discusses how one agency is using data analytics with information collected through conflict of interest and private interest declarations.

CONFLICT OF INTEREST PROCEDURES THAT FACILITATE FURTHER ANALYSIS

Case study 9

Consistent with the VPSC's Model Policy, one Tier 1 agency requires all staff to declare any potential, perceived or actual conflicts of interest, and certain staff to declare private interests on appointment, annually and within five working days if their circumstances change. These declarations are assessed by the agency's audit and risk committee, and all declarations and employee attestations are recorded on a central risk register which is reviewed annually.

The agency also uses a data analytics tool to monitor declared conflicts of interests. The agency uses a system that collates, tracks and compares employee data and declarations. This data includes information from employee attestation or conflict of interest documents, and is compared to complaints received about employees or pending investigations. Only compliance officers and managers overseeing investigations have unlimited access to data within this system.

3.2.6 Hiring friends or family for a government job

Perceived risk

Eight agencies stated hiring friends or family for a government job posed a great risk to their organisation. A further 24 agencies stated this risk was relevant to their organisation to some extent, while six did not consider it a risk to their organisation at all.

Three of the six agencies that did not consider the issue to be a corruption risk to their organisation advised that controls were partly or comprehensively in place to manage this risk. These agencies may therefore consider there to be no residual risk.

Of the 32 agencies that consider hiring friends or family for a government job posed a risk to their organisation, 11 indicated the risk was not recorded in their risk registers or that the survey question was not applicable. However, all 11 indicated controls were partly or comprehensively in place to manage this risk.[64]

Controls

Irrespective of whether agencies considered hiring friends or family for a government job to be a corruption risk to their organisation, 34 agencies said their organisation had controls partly or comprehensively in place to manage the risk. Twenty-five described specific controls including:

- Policies and procedures: such as codes of conduct and policies on recruitment and selection, merit, secondment and redevelopment, secondary employment, probity and conflict of interest, pre-employment screening, delegations, and protected disclosures, as well as the VGPB procurement guidelines, and employment principles set out in the *Public Administration Act 2004*.[65]
- Training and communication: such as ongoing awareness programs and communication to employees in relation to the policies discussed above.[66]

[64] One further Tier 3 agency that considered this issue a risk 'to some extent' did not respond to questions regarding controls or recording of the issue in its risk register.

[65] 19 agencies from all three tiers.

[66] Eight agencies from all three tiers.

- Conflict of interest declarations: with reference to registers in place and requirements that employees declare conflicts if they are on recruitment selection panels.
- Delegation of authority/multi-level approvals: primarily through human resource delegation policies and procedures, multi-member interview and selection panels. For example, reflecting the employment principles set out in the Public Administration Act, one agency advised its competitive employment practices included 'double interviews by multi-member interview panels'.[67]
- Management oversight: for example, one agency commented the organisation has executive management oversight for all recruitment, while another discussed involvement of and escalation to the parent department if any concerns are raised during recruitment.[68]
- Internal reconciliation and review: for instance, one agency commented it is implementing data analytics to support other controls aimed at managing this risk.[69]

In consultations, agencies also discussed how a robust recruitment process could assist in managing the risk of 'hiring friends or family for a government job', as noted in the following case study.

EMPLOYMENT CONTROLS

Case study 10

A Tier 1 agency advised it conducts an extensive screening process for prospective employees. All offers of employment are conditional upon successful completion of a conflict of interest declaration, a national police check, and verbal reference checks. Shortlisted candidates are required to comply with additional qualification checks, including evidence of their qualifications in the form of original documentation, where a qualification, licence or accreditation is nominated as a requirement of the role. Senior and high-risk roles are required to complete pecuniary interest declarations and disclose concurrent executive or non-executive roles upon appointment. Employees are also re-screened upon promotion.

The principle of merit-based and competitive recruitment is well established in the Victorian public sector. Under the Public Administration Act, public agency heads are required to ensure employment decisions are merit based, while the VPS Code of Conduct requires that public officers make decisions impartially – including decisions about employment. However, as noted in IBAC's 2018 report on employment-related corruption and misconduct risks,[70] corruption vulnerabilities are present at different stages of the employment life cycle. For instance, IBAC research has identified internal applicants are not always subject to the same probity rigour as external applicants. This is concerning because once within an organisation, an individual may move to a higher-risk position without undergoing adequate screening.[71]

[67] Six agencies from all three tiers.

[68] Two Tier 1 agencies.

[69] One Tier 3 agency.

[70] IBAC 2018, *Corruption and misconduct risks associated with employment practices in the Victorian public sector*, Melbourne.

[71] IBAC 2018, *Corruption and misconduct risks associated with employment practices in the Victorian public sector*, Melbourne, p.12.

Employee screening and due diligence should be considered for all prospective candidates, as well as re-screening for employees moving to a position considered to be high risk in terms of potential exposure to fraud and corruption. The objective of the screening process is to confirm the background, integrity, identity and credentials of the candidate, and mitigate potential risks of fraud and corruption to the organisation. The process should also consider regular reviews of positions with these particular risk exposures, as well as any changes in the personal circumstances of an employee.

In October 2018 the VPSC issued a new employment screening policy for VPS executive officers, partly in response IBAC's Operation Lansdowne.[72] The policy requires all preferred candidates for VPS executive positions to complete a statutory declaration in relation to relevant instances of misconduct, and to sign a consent form allowing the prospective employer to contact the candidate's current and previous employers to substantiate their employment history.[73]

3.2.7 Abuse of discretion

Perceived risk

Five agencies stated abuse of discretion posed a great risk to their organisation. A further 25 stated this risk was relevant to their organisation to some extent, while seven stated it was not a risk to their organisation at all. One agency did not respond to questions regarding the risk of abuse of discretion.[74]

In consultations, one of the agencies that stated abuse of discretion was not a corruption risk clarified that it had controls in place to manage that risk, as discussed in the following case study.

DISCRETION CONTROLS

Case study 11

One Tier 2 agency noted that certain designated employees made decisions about resource allocation and entitlements and discussed how this posed a risk of abuse of discretion for the organisation. To prevent insider trading, all staff on that team are required to make declarations about their trading decisions, however declarations are held by one manager. From a risk perspective, this control could be strengthened by involving more than one manager and having some form of central oversight in place.

Another agency that did not consider abuse of discretion to be a risk to their organisation noted the controls they have in place to manage this risk 'leave the agency with no room or opportunity' for abuse of discretion. The agency advised the controls included laws and regulations governing operations and a process of sourcing independent legal advice from the Victorian Government Solicitor's Office.

Two other agencies that did not consider abuse of discretion to be a corruption risk to their organisations also said the risk was partly or comprehensively recorded on their risk registers with controls in place to manage this risk. This may indicate these agencies do not consider abuse of discretion a corruption risk based on the level of residual risk given the controls in place.

Of the 30 agencies that considered abuse of discretion posed a risk to their organisation, seven indicated the risk was not recorded in their risk registers. However, these agencies also indicated controls were partly or comprehensively in place. While most agencies did not provide specific reasons for their response, one agency noted abuse of discretion was considered a relatively small risk due to the nature of its work (professional services) and controls in place (primarily multi-level approvals).

[72] IBAC 2017, *Operation Lansdowne: An investigation into allegations of serious corruption involving Victorian vocational education and training, and public transport sectors*, Melbourne.

[73] VPSC 2018, *Executive Re-employment Screening Policy, VPSC*, Melbourne.

[74] One Tier 3 agency.

Controls

Regardless of whether agencies considered abuse of discretion to be a corruption risk to their organisations, 33 said their organisation had controls partly or comprehensively in place to manage the risk. Twenty-five described specific controls including:

- Policies and procedures: for example, policies around financial and human resource delegations, fraud and corruption, procurement and expenditure, and codes of conduct.[75]
- Delegation of authority/multi-level approvals: for example, one agency said it had a comprehensive deed of delegation outlining management's accountabilities for discretionary decisions.[76]
- Training and communication: such as financial management/delegations training for employees with financial delegations, and induction program content to inform new staff of the agencies' financial delegations policy.[77]
- Segregation of duties: for example, one agency advised authorised officers have limited discretion in deciding enforcement actions because line managers are required to authorise decisions, which may also be reviewed by a formal panel of legal and senior management representatives.[78]
- Internal reconciliation and review: such as performance reviews and data analysis.

Other general controls listed included audit activities,[79] robust recruitment processes,[80] and system controls.[81]

To ensure delegation mechanisms operate as an effective control of abuse of discretion, good practice would include agencies:

- conferring delegations of authority on roles or positions rather than individuals
- reviewing delegations regularly and conducting checks to ensure approval workflows and access to systems are based on approved levels of delegation
- ensuring when staff change roles or leave the agency, delegations are reviewed and approved by appropriate personnel, and previous delegations are promptly updated or removed.

3.2.8 Improper funding arrangements and/or use of grants

Perceived risk

Three agencies stated improper funding arrangements and/or use of grants posed a great risk to their organisation. A further 19 agencies stated this risk was relevant to their organisation to some extent, while 16 agencies stated it was not a risk to their organisation at all.

Six of the 16 agencies that did not consider the issue to be a corruption risk to their organisation said controls were partly in place to manage this risk. This may indicate these agencies do not consider the risk relevant to their organisations based on the level of residual risk given the controls in place. For instance, one agency commented this was not a risk because 'funding is provided in the form of a Special Appropriation from Treasury … [and the agency] does not receive grants or any other forms of revenue for operational purposes'.

The other 10 agencies responded 'no' or 'not applicable' to the survey questions regarding recording the issue on their risk registers or having controls, suggesting their operations may not involve funding arrangements or grants.

[75] 15 agencies from all three tiers.
[76] 13 agencies from all three tiers.
[77] Eight agencies from all three tiers.
[78] Five agencies from all three tiers.
[79] Two Tier 2 agencies.
[80] A Tier 1 agency.
[81] A Tier 3 agency.

Of the 22 agencies that considered improper funding arrangements and/or use of grants posed a risk to their organisation, six indicated the risk was not recorded in their risk registers. However, all six indicated controls were partly or comprehensively in place to manage this risk.[82]

Controls

Irrespective of whether agencies considered improper funding arrangements and/or use of grants to be a corruption risk to their organisations, 26 agencies said their organisation had controls partly or comprehensively in place to manage the risk. Sixteen of these agencies described specific controls including:

- Delegation of authority/multi-level approvals: specifically, the approval of funding and/or grants by appropriate levels of delegations.[83] For example, two agencies noted grant approvals were signed by the relevant Minister.
- Policies and procedures: such as codes of conduct, policies governing procurement, gifts, benefits and hospitality, conflict of interest, capital expenditure, purchasing, fraud and corruption control, and financial management.[84]
- Audit activities: such as internal and external audit programs concerning funding arrangements.[85] For example, one Tier 2 agency said funding was usually subject to high levels of scrutiny from relevant departments.
- Fund/grant reporting: reporting and acquittal of funds or grants including reporting requirements specified in the funding agreement.[86]
- Internal reconciliation and review: for example, one agency noted it had 'monthly monitoring of budget expenditure by program areas', while another noted 'monthly financial reconciliations are in place'.[87]
- Management oversight: such as oversight of research projects by a 'research and ethics' office or committee, and approval of grants by a governance committee.[88]
- Training and communication: such as employee training and/or ongoing awareness programs and communication to staff.[89]

GRANT FUNDING CONTROLS

Case study 12

One department said the vast majority of grants were administered by its portfolio agencies. The department has established grant panels that track milestones for grant payments, and requires evidence and receipts to be provided before any reimbursements or payments are made. To monitor and control potential fraud or corruption risks, larger value grants require a physical inspection of sites where grants have been applied, and the department has a right to recoup funds if the item in the grant is not delivered.

[82] One further Tier 3 agency that considered this issue a risk 'to some extent' did not respond to questions regarding controls or recording of the issue in its risk register.
[83] Eight agencies from all three tiers.
[84] Seven agencies from all three tiers.
[85] Seven agencies from all three tiers.
[86] Six agencies from all three tiers.
[87] Two Tier 2 agencies.
[88] Two Tier 2 agencies.
[89] Two Tier 2 agencies.

3.2.9 Bribery

Perceived risk

Two of the 38 agencies stated bribery posed a great risk to their organisation. A further 30 agencies stated this risk was relevant to their organisation to some extent, while six stated bribery was not a risk to their organisation at all.

Of the six agencies that said they did not consider bribery to be a corruption risk in response to the survey:

- Two agencies noted the risk was recorded on their risk registers at least in part, and both agencies considered comprehensive controls were in place to manage bribery risks. However, in consultations, one of these agencies advised it *did* consider bribery a corruption risk and it had controls in place to manage that risk.
- One agency noted while the risk was not recorded on its register, controls relevant to the management of this risk were partly in place. The agency also advised bribery is identified as a risk in the context of fraud and corruption, for example in the agency's fraud and corruption control policy and plan.
- Three agencies noted the risk was not recorded on their risk registers:
  - one noted while the term 'bribery' was not used, 'collusion and corruption' was identified as a key category in its fraud risk register to capture this risk
  - a second noted bribery was now expressly included in its gifts, benefits and hospitality policy
  - the third explained bribery was not recorded in its risk register because it did not present a significant risk. This agency advised while specific controls had not been employed to address the risk of bribery, broader measures (including controls around decision-making, finance and procurement; gifts, benefits and hospitality; requirements to declare private interests; and activities designed to encourage staff to report concerns) serve to monitor the risk and detect potential instances of bribery.

Of the 32 agencies that considered bribery was a risk to their organisations, eight indicated the risk was not recorded in their risk registers. These agencies did not specifically explain why but all eight indicated they had partial or comprehensive controls to mitigate the risk, while some said bribery was not included in risk registers because of very limited risk due to the nature of their business. For example, one agency commented:

'… the business of [the agency] involves providing professional services … for government clients, departments and agencies. The exercise of powers and discharge of functions is undertaken pursuant to requests for assistance from clients. The scope for possible bribery exists in the knowledge that those services will usually form the basis of action taken by the client. In this respect, there is the potential to influence an exercise of power. However, those communications are always subject to multiple reviews by other staff members. Accordingly, the scope for bribery is very small.'

Controls

Irrespective of whether agencies considered bribery to be a corruption risk to their organisation, 35 agencies responded they had controls partly or comprehensively in place to manage the risk. Twenty described specific controls including:

- Policies and procedures: such as fraud and corruption policy, code of conduct, conflict of interest policy, gifts, benefits and hospitality polices.[90]
- Training and communication: such as staff induction, annual refresher training, and other ongoing awareness programs and communication to employees.[91]
- Segregation of duties: especially in relation to procurement and transaction processing.[92] For example, one agency commented there had been instances of offers of bribes to officers, however the risk is mitigated by having inspections performed in pairs, and in some instances using a pool of available inspectors.
- Audit activities: such as internal and/or external audit activities however, agencies did not specify how audit activities had been developed to identify bribery risks.[93]
- Processes to declare and register conflicts of interest and gifts offered:[94] for instance, one agency's gifts and benefits policy provided line management accountability by specifying who the CEO, Commissioner and Chair must obtain approval from before accepting hospitality. The agency also publishes its gifts and benefits register for the current and previous financial year on its website. The register notes who made the offer, the value, the cumulative value from the same source, and whether the item was accepted or declined.
- Reporting avenues: for example, one agency had a provision in its gifts, benefits and hospitality guideline requiring any bribery attempt to be reported to the CEO, while another operated an external disclosure service for employees to report anything suspicious.[95]
- Internal reconciliation and review: to ensure procedural integrity and mitigate exposure to bribery risks, one agency implemented a detailed, automated internal reporting and reconciliation process, and another stated it had automated its systems to minimise misuse of relevant program funds.[96]
- Delegation of authority/multi-level approvals:[97] for example, one agency commented the services it provides are generally subject to multiple levels of reviews and approvals, which is an element of its mitigation strategy in relation to the risk of bribery.
- VGPB requirements: one agency identified the contractual requirement for suppliers/contractors to comply with the supplier code of conduct as a bribery control mechanism, noting the code requires suppliers to comply with all anti-bribery and anti-corruption laws.[98]

90 13 agencies from all three tiers.
91 Six agencies from all three tiers.
92 Four agencies from all three tiers.
93 Four agencies from Tiers 1 and 2.
94 Three agencies from Tiers 1 and 2.
95 Two Tier 2 agencies.
96 Two Tier 1 agencies.
97 Two agencies from Tiers 1 and 2.
98 One Tier 2 agency.

3.2.10 Other corruption risks

Perceived risks

Agencies were asked to nominate other corruption risks they considered relevant to their organisations. Corruption risks cited included:

- kickbacks
- favouritism
- abuse of role/function for personal benefit
- third-party collusion
- misuse of confidential information
- cyber risk
- payroll fraud
- theft or misuse of physical assets
- fraudulent leave, overtime, entitlements and expense claims
- organised crime infiltration.

It is noted there is some overlap between these corruption risks and those discussed earlier in this report. However, the review identified instances where agencies may have adopted a narrow definition of corruption risks when identifying relevant risks, as discussed in the following case study.

RECOGNISING AND ADDRESSING RISKS AS CORRUPTION RISKS

Case study 13

One Tier 2 health sector agency explicitly stated it did not consider theft of drugs to be a corruption risk.

During the consultations, agency representatives noted there had been an incident within the past five years of staff stealing prescription medication from a health-care facility. The issue was characterised as a performance risk and not a corruption risk. However, the agency subsequently advised this did not accurately reflect its views of corruption, and noted the agency's process would be to report the matter to the appropriate authorities.

The view that theft of drugs does not constitute a corruption risk is at odds with observations made in IBAC's Operation Tone, which investigated a number of allegations including that Ambulance Victoria paramedics stole, trafficked and/or used Ambulance Victoria drugs of dependence.[99]

In 2018, the Western Australian Corruption and Crime Commission raised similar concerns that drug discrepancies had sometimes been treated as a welfare or human resources issue by WA Health, making it difficult to identify the reason for the discrepancy and deal with potential theft appropriately, namely by way of criminal or disciplinary processes.[100]

Information provided by agencies during this review suggests there continues to be a strong focus on financial management and the financial impact of potential corruption risks, although recognition of the need to consider a broader range of corruption risk factors is increasing. Participating agencies across all three tiers are considering a range of controls to address these risks. These efforts could be supported through better recording of issues in risk registers to ensure corruption risks and controls are formally considered and reviewed on a regular and structured basis.

[99] IBAC 2017, *Operation Tone: Special report concerning drug use and associated corrupt conduct involving Ambulance Victoria paramedics*, Melbourne.

[100] WA Corruption and Crime Commission 2018, *Report on serious misconduct risks around dangers drugs in hospitals*, Perth.

4 Ethical culture and leadership

4.1 Governance

4.1.1 Implementing and maintaining an integrity framework

The Standard notes the implementation of an integrity framework, as well as a process of endorsing, benchmarking and monitoring such a framework, can help to manage the risk of fraud and corruption within an organisation, as well as guiding the development of an organisation's ethical culture.

According to the Standard, an integrity framework should include:

- Example setting: Senior managers should lead by example, by modelling expected standards of behaviour and complying with the various elements of the organisation's integrity framework.
- Senior management recognition: Senior managers should recognise and regularly promote the importance of an ethical culture.
- Reporting of complaints: It is critical organisations have a clear mechanism to report ethical concerns regarding the organisation, both for external and internal complaints.
- Code of behaviour: Organisations should implement codes of conduct that incorporate a high-level aspirational statement of values and more prescriptive actions to support a culture of integrity.
- Allocation of responsibility: A senior officer should have clear responsibility for ensuring the organisation's integrity initiatives are implemented and monitored.
- Ethics committee endorsement: There is value in a committee or dedicated forum that provides authoritative advice on integrity issues that cannot be resolved by a line manager.
- Communication: There should be a program for regularly communicating the organisation's code of conduct.
- Training: It is important to provide specific, ongoing training on the code of conduct, and fraud and corruption awareness.
- Performance management reinforcement: There is value in incorporating ethical standards in performance assessment systems, remuneration strategies and employee feedback.
- Benchmarking: Analysis of ethical standards over time can help identify improvements in an organisation's integrity standards.
- Compliance: Organisations may require all employees to sign an annual declaration that they have complied with all integrity policies, including those concerned with conflict of interest, disclosure of information, and other integrity-related matters.

An integrity framework should also include robust risk management process, and fraud and corruption control frameworks to identify and address corruption risks.

4.1.1.1 Policies

Recognising agencies may take different approaches to address key elements of their integrity framework, agencies were asked, as part of this review, to nominate the primary policy documents in place to govern integrity and guard against fraud and corruption.

The documentation provided by agencies suggests most have developed a range of integrity framework policies that generally include a fraud and corruption control policy, code of conduct, conflict of interest policy, gifts, benefits and hospitality policy, supplier engagement policy, and protected disclosure policy. In addition, a small number provided documentation of a dedicated integrity framework they have in place.[101]

Several agencies also provided further policies regarding financial risks for consideration including a financial delegations policy, cash and treasury policy, and expenditure policy,[102] rules for financial management,[103] and a financial code of conduct.[104]

4.1.1.2 Practices

In consultations, several agencies with more mature integrity frameworks indicated they had developed additional material within their overarching framework. For example, supplementary material developed by a Tier 1 agency included integrity evaluation plans, integrity compliance strategies, risk management strategies, and recruitment policies. A Tier 2 agency noted it had developed polices relating to fair treatment, bullying prevention, and workplace dispute resolution strategies. These organisations prioritised integrity initiatives and allocated full-time resources to the development of their integrity framework, including fraud forums and dedicated forensic teams.

DEVELOPMENT AND COORDINATION OF INTEGRITY FRAMEWORK DOCUMENTATION

Case study 14

Following the Victorian Secretaries Board's 2016 communique outlining its commitment to strengthen integrity throughout the Victorian public sector, a Tier 3 agency created an integrity framework document in early 2018, to consolidate existing and new elements of its integrity framework (policies, tools and communications, among other elements). That overarching integrity framework covers the following elements and was developed with reference to IBAC resources and through consultations with other agencies:

- conflict of interest policy
- gifts, benefits and hospitality policy
- fraud and other losses policy
- disclosure of related party transactions
- ethical leadership development program
- 'Speak Up' program to encourage reporting
- internal compliance framework
- risk policy and management framework
- procurement framework
- human resource management.

[101] Two Tier 1 agencies and two Tier 3 agencies.

[102] Tier 1 agency.

[103] Tier 2 agency.

[104] Tier 3 agency.

4.1.1.3 Clear governance between departments and portfolio agencies

The 2014 review identified a possible disconnect between departments and their portfolio agencies, in that each could consider the other responsible for a particular aspect of integrity. This suggested room for improvement in the relationship between departments and agencies in terms of governance and integrity.

It is clear departments play an important role in guiding and supporting their portfolio agencies, which may have limited resources. In relation to governance and integrity, this guidance and support might include:

- Sample integrity-related policy and procedures templates. For example, one department advised it provides a fraud and corruption framework template for portfolio agencies.
- Guidance on high corruption risk areas and suggested controls.
- Training and communication related to integrity topics.
- Creating discussion platforms for relevant roles in portfolio agencies to exchange ideas related to corruption prevention, detection and response, such as an email list of integrity professionals in portfolio agencies whom staff can consult and seek advice.
- Involvement in corruption prevention forums and seminars. For example, one Tier 2 agency regularly participated in a national fraud forum involving participants from agencies with similar profiles. The agency noted this forum was a way to raise staff awareness about fraud and corruption risk and integrity issues common to these organisations.

Several departments advised they had provided portfolio agencies with formal and/or informal support and guidance to develop integrity frameworks, recognising regional and smaller portfolio agencies may have limited resources.

DEPARTMENTAL ASSISTANCE TO PORTFOLIO AGENCIES

Case study 15

A department advised it provided portfolio agencies with templates and guidelines on preventing and detecting fraud and corruption in response to requests from the agencies and investigation results.

For example, in March 2017 a 'Fraud, Corruption Control and Protected Disclosures Framework' template was prepared by the department's central integrity unit and sent to portfolio agencies for reference. More recently, the department provided portfolio agencies with guidelines detailing examples of good and bad practices, and discussed controls that should be in place to manage executive expenses, following recommendations made by IBAC.

4.1.2 Senior management commitment to controlling the fraud and corruption risks

According to the Standard, senior managers should have a high level of awareness of the risks of fraud and corruption within their organisations, and a clear commitment to controlling those risks. Corrupt conduct can go undetected if senior managers neglect to promote integrity, fail to treat corruption risks as a serious threat, or fail to allocate adequate resources to managing those risks.

It is good practice, according to the Standard, for senior managers to understand fraud and corruption issues including the types of fraud and corruption common within the VPS, and their organisation's fraud and corruption prevention and control strategies.

The Standard also advises it is good practice to have a dedicated senior management group that communicates the need for corruption awareness and prevention, preferably before a major incident occurs and serious financial and reputational damage incurred.

This review indicated senior management commitment to controlling fraud and corruption risk was generally well documented by participating agencies. Policies included statements of commitment to the implementation and oversight of integrity initiatives, and strong messaging that senior management has ultimate responsibility to promote a culture of compliance in this area. Fraud and corruption control policies and codes of conduct provided by agencies described in detail the roles and responsibilities of each level of executive and line management.

Consultation with selected agencies provided assurance that senior management within those agencies were committed to the promotion of integrity and an ethical culture. Many participating agencies have dedicated fraud and corruption teams in the form of panels, forums, and/or decision-making committees to provide oversight of the organisation's integrity framework and ongoing benchmarking of ethical standards.

Agencies were asked to describe the various ways in which their senior management promotes corruption prevention and integrity. To provide some guidance to agencies, they were provided with five examples which were broadly reflected in agency responses.[105] Agencies indicated that their senior management promotes integrity in a number of ways. This included 10 agencies that have specific committees or forums dedicated to risk and/or integrity matters. Encouraging staff to report concerns and behave with integrity, and responding in an appropriate and visible manner to reports or issues raised were also identified as ways in which agencies promote corruption prevention and integrity.[106]

Other ways agencies said they promote corruption prevention and integrity were:

- Training: including induction for new employees, and fraud and corruption awareness training.
- Communication: including newsletters, reminder emails, intranet articles, posters and other campaigns to encourage staff to report concerns and behave with integrity.
- Policies: including framework resources and programs that promote integrity in the workplace.
- Groups and networks: including developing local integrity champion networks or designating individuals to have a specific role or responsibility for promoting staff awareness of corruption risks.
- Declarations and attestations: in relation to knowledge of and compliance with codes of conduct, conflict of interest or private interest declarations.[107]
- Human resource activities: for example, by including integrity criteria in position descriptions, performance plans,[108] and recruitment policies.

Thirty agencies advised they have a dedicated team or committee of employees with responsibility for corruption prevention measures. In particular, 13 agencies noted the organisation's investment in such a team or individual is one way in which senior management actively promotes corruption prevention and integrity measures, although one noted a team of three executives is responsible for fraud management (not integrity or corruption).

Several specific measures used to promote integrity are discussed in detail on the following pages.

[105] The five examples provided in the survey were:
- the attendance of the compliance manager at all relevant Executive Committee meetings
- receiving and acting upon reports (rather than simply 'noting' them)
- encouraging staff to report concerns via emails, all staff meetings etc
- demonstrated use of compliance expertise
- a program of strategic anti-corruption activities.

[106] 17 agencies indicated acting on reports and issues raised is one of the ways senior management promotes integrity, while 16 indicated senior management encourages staff to report concerns and/or behave with integrity.

[107] Discussed further in section 4.1.2.2.

[108] Discussed further in section 4.1.2.1.

4.1.2.1 Integrity-related performance measures

Half of the participating agencies indicated integrity is considered in employee performance reviews or appraisal mechanisms in some way, however responses suggested agencies generally find it difficult to *measure* integrity-related KPIs.

Only one agency stated integrity-related measures are included in executive performance plans. However, another agency noted during performance reviews, executives are held to KPIs that measure integrity.

Integrity-related behaviours could be considered in employee performance reviews, as a stand-alone criteria or in terms of the organisation's values. Incorporation of integrity-related behaviours in performance reviews might include:

- baseline requirements to complete mandatory integrity training and/or declare compliance with integrity-related polices in order to access performance-related progression payments
- KPIs for managers on how staff in the team have completed training activities
- recognition of individuals who display integrity in exceptional ways.

Twelve agencies indicated they have a performance measure for integrity in their organisation's business plan, planning strategy or work program. For instance:

- one agency stated measures are included in executive performance plans[109]
- nine referred to work programs including training, integrity programs, internal audit or other reviews of risk areas, as ways in which senior management actively promotes corruption prevention and integrity, but none appeared to relate directly to the measurement or monitoring of integrity.

The VPSC plans to develop a new executive performance framework, which agencies may wish to consider in developing integrity measures for executive officers.[110] IBAC understands the framework will set out performance expectations for all executive officers in the VPS, with reference to the VPS Code of Conduct and public sector values and behaviours.[111]

Twenty agencies said they have integrity measures in staff performance reviews or appraisal mechanisms:

- Four agencies identified this as a way in which senior management actively promotes corruption prevention and integrity, for example:
  - one agency noted 'conflict of interest declarations are part of performance process', adding their performance development plan formally asks employees every six months to indicate whether they have any interests they need to declare
  - another advised that its employees are assessed in performance reviews on their compliance with their integrity measures, and executives are held to KPIs to measure their compliance with these measures. For example, the CEO has a KPI to maintain fraud and corruption risk management initiatives.
- Three agencies noted that having integrity measures in staff performance reviews or appraisal mechanisms is an effective way senior management can assure itself integrity is promoted, and employees have a good understanding of and confidence in the organisation's corruption prevention measures.

However, agency responses also suggested they generally find it difficult to implement and measure integrity-related KPIs.

[109] Tier 3 agency.

[110] Victorian Public Sector Commission 2018, *Strategic Plan to 2020*, Melbourne, p.15.

[111] DPC update in response to Operation Ord recommendations, July 2018, published on IBAC's website: www.ibac.vic.gov.au/docs/default-source/responses/summary-of-dpc-july-2018-update-in-response-to-operation-ord-recommendations.pdf?sfvrsn=933e7575_0

Possible integrity-related KPIs agencies could consider for managers include:

- KPIs for managers on how many staff in the team have satisfactorily completed integrity related training
- participation in integrity-related activities
- recognition of individuals who display integrity in ways that go beyond what is expected of them in their day-to-day roles
- regular discussions around the agency's values and code of conduct
- exploring other opportunities to embed integrity in how staff carry out their duties.

4.1.2.2 Declarations and attestations

The Standard suggests a strong integrity framework should include a requirement for all employees to sign an annual declaration that they have complied with all relevant integrity policies including conflicts of interest, disclosure of information, and other integrity-related matters. Declarations can help to identify risks that need to be managed, and encourage employees to think about their responsibility to act with integrity.

Declarations required of employees (and prospective employees) may relate to:

- preferred candidates to provide information about any history of misconduct[112]
- relevant qualifications for preferred candidates
- gifts, benefits and hospitality offered, declined, accepted and provided
- private interests (annually and as they occur)
- secondary employment (annually and as it occurs).

In addition, any employees involved in panel and evaluation arrangements (eg in relation to procurement, recruitment, grants, funding, licensing and qualification review panels among other things) should declare any actual, potential or perceived conflicts of interest.

Twenty-eight agencies said their employees are required to periodically sign a statement of acknowledgement and commitment to relevant integrity-related policies, including eight agencies that advised all staff are required to make a declaration in relation to conflicts of interest, private interests and the code of conduct. Twenty agencies stated only some staff were required to make a declaration, that is, declarations were variously required from some senior executives, board members, managers, staff with financial delegations, and/or members of tender evaluation panels.[113]

Fifteen agencies advised declarations are refreshed at least annually. For example, a Tier 2 agency noted its refresher training is conducted via an online training module which guides staff to relevant fraud and corruption policies and guidelines, then requires staff to acknowledge they have accessed and read those documents. Other agencies noted staff must sign an acknowledgement of policies when they commence with the agency, but did not indicate whether these acknowledgements were periodically refreshed.

An agency's position on corruption and integrity can also be promoted more broadly by requiring declarations from contractors and suppliers around personal, financial, business or other relationships with current employees. This can also help to facilitate timely management of potential conflicts.

[112] Effective October 2018, all preferred candidates for VPS executive positions are required to sign a statutory declaration declaring relevant instances of misconduct, and a consent form allowing the prospective employer to validate the declaration with previous employers. Victorian Public Sector Commission Circular 2018-05, VPS *Executive Pre-employment Screening Policy*.

[113] The remaining 10 agencies advised staff are not required to make any such declaration.

Electronic management of declarations is good practice. It reduces the chances of mistakes or omissions by avoiding the need to transfer data from one to another. Storing of structured data in a central repository also allows for easy analysis and cross-checking. When declarations are stored in a way that is easy to analyse electronically, agencies can check across gifts and benefits, and private interests registers to identify whether employees have declared and managed conflicts that may affect integrity during activities such as recruitment and tender evaluation. Agencies can also perform data analyses to better understand trends and respond quickly to emerging risks when they arise. For example, one Tier 2 agency advised declarations of gifts offered, declined and received are analysed to understand whether policies and processes need be updated to address certain types of gifts offered to employees, and to identify suppliers who frequently offer gifts.

Agencies should also consider requiring all employees to make a declaration at key points in certain processes (eg procurement and recruitment) such as when a panel is set up, a decision is about to be made and as part of an annual declaration process. To ensure the process is complete and transparent, if an employee does not have any private interests that warrant declaring, they should state they have nothing to declare rather than not submitting a declaration.

4.1.3 Assurance that integrity is promoted and understood

Across all participating agencies, the top three ways in which senior management assures itself integrity is promoted within their organisations, and employees have a good understanding and confidence in corruption prevention measures are: leading by example, training, and support for audits and other reviews that examine compliance with integrity-related policies.

While reports of suspected corruption were also identified as a means of assurance, agencies had mixed views in terms of whether a larger or smaller number number (or even zero) reports of suspected corrupt conduct provided assurance that integrity was promoted and understood. For example, two agencies referred to the 'number and nature of reports' received without providing further context about whether a high or low number of reports was considered to provide assurance,[114] while another agency stated 'zero reported corruption incidents' was an effective way of providing such assurance to senior management.[115] While low numbers may suggest a strong culture in which no incidents of suspected corruption occur, they may also suggest a lack of willingness to report issues.

A number of agencies also noted participation in the VPS People Matter Survey and other internal questionnaires helped them gain insight into employees' perceptions of corruption, and willingness to escalate or report issues including suspected fraud and corruption.[116]

Surveys can help identify areas where further integrity initiatives may be needed, and tailor strategies to effectively address staff concerns and misconceptions. For example, Figure 2 outlines responses to two questions from IBAC's 2017 survey of Victorian state government employees. These responses suggest while the majority of respondents were willing to report if they observed corruption, only one third were confident they knew how to report corrupt conduct.[117] These results were drawn from a broader cross-section of state government agencies, some of which were not involved in this review. However, they suggest that there may be value in organisations developing strategies to bridge this gap between willingness to report and confidence to make a report.

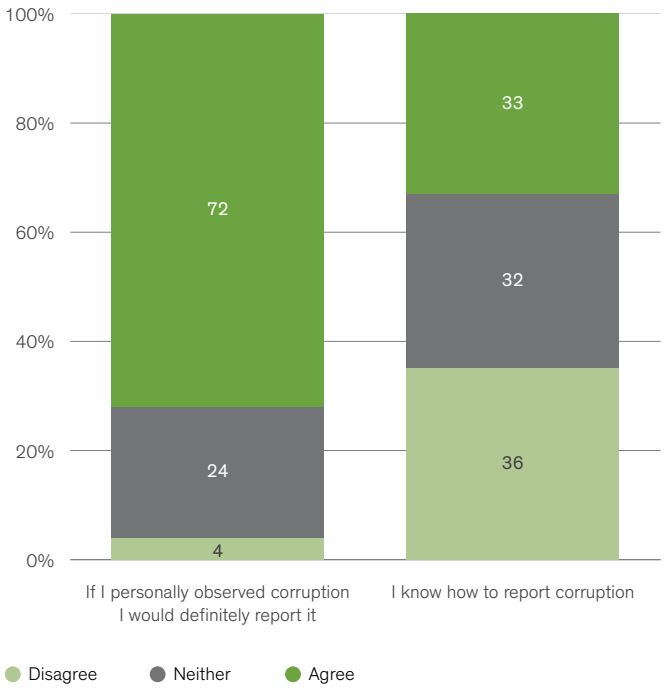
[114] A Tier 2 and a Tier 3 agency.

[115] A Tier 1 agency.

[116] A Tier 1 and a Tier 2 agency.

[117] IBAC 2017, *Perceptions of corruption, Survey of Victorian state government employees*, Melbourne, p.12. Note that the data for the question 'I know how to report corruption' (shown in Figure 2) was only partially reported by IBAC in its 2017 report. Note that number in Figure 2 may not total 100 due to rounding.

FIGURE 2: 2017 STATE GOVERNMENT EMPLOYEE PERCEPTIONS OF CORRUPTION



n = 4542, figures may not total 100 due to rounding

4.2 Communication and awareness

According to the Standard, organisations should demonstrate that every employee (management and non-management) is generally aware of fraud and corruption and how to respond if it is detected or suspected. Organisations should regularly communicate to their staff about what constitutes fraud, corruption and prevention/detection measures, and importantly, that such conduct will not be tolerated.

Consistent with the Standard, an organisation's fraud and corruption framework should note whether:

- all appropriate employees receive training in the organisation's code of conduct and other elements of the integrity framework, at induction and throughout their employment
- all employees receive regular fraud and corruption awareness training appropriate to their level of responsibility
- updates and changes to fraud and corruption-related policies, procedures, code of conduct and other integrity-related matters are effectively communicated to all employees
- staff are aware of the ways they can report allegations or concerns regarding fraud or corrupt conduct
- staff are encouraged to report any suspected incidence of fraud or corruption.

Additionally, fraud and corruption awareness and standards of conduct should be supported through regular meetings within business units, internal publications and through the overt, ongoing commitment demonstrated by senior management.

Documentation provided by the majority of Tier 1 and Tier 3 agencies stated the importance of having a fraud and corruption communication plan, and set out details of fraud and corruption in-house awareness training, campaigns, and e-learning initiatives to strengthen awareness throughout the organisation. Many Tier 2 agencies provided examples of the types of integrity messages they communicate to staff, but did not provide evidence of a communication strategy or otherwise demonstrate agency-wide communication and awareness of fraud and corruption among staff.

Examples of communication and awareness material provided by agencies included induction training on corruption, ongoing training and awareness programs, regular distribution of code of conduct policies, conflict of interest declarations, and/or probity training.

Communication and awareness-raising strategies around fraud and corruption should enable employees to identify potential fraud and corruption, and explain the reporting process so that staff know how to report suspected corrupt conduct and have confidence in the process.

4.2.1 Employee education and communication

The 2014 review found relatively few public bodies reported having specific education or training programs with corruption-specific information. A few agencies indicated they were developing fraud and corruption awareness training modules.

Based on agencies' responses to this review, it is clear that since the 2014 review, most agencies across all tiers have implemented dedicated corruption and integrity training for employees. The vast majority of agencies stated they provide their employees with some form of education related to corruption through dedicated or other training with corruption elements. For agencies that do not yet have specific corruption training as a dedicated program or embedded training, corruption-specific and relevant materials are being considered.

The 2014 review noted that most agencies referred to the VPS Code of Conduct as the subject of employee training about corruption. However, at the time, it was noted the VPS Code of Conduct contained very little specific information about corruption. In this review, although the VPS Code of Conduct training was sometimes referenced by agencies, they also reported providing other, dedicated corruption training.

Agency responses included a number of interesting corruption education and training initiatives such as:

- Face-to-face training, online modules, and interactive activities. For example, one Tier 2 agency held an 'internal forensics expo' which provided information to staff on potential fraud threats to the agency. A Tier 1 agency used bingo to test attendees' comprehension of the topics discussed in the fraud and corruption training, and to keep them engaged.
- Inviting contractors, suppliers and other external target audiences to receive training on the agency's integrity framework.
- Engaging subject matter experts to develop and deliver training on internal and/or external risk and compliance.

IBAC has a range of useful resources on its website that provide information to the Victorian public sector and the community to share lessons about corruption vulnerabilities and prevention measures. Agencies said they found case studies and real life examples demonstrating corruption risks, effective use of controls and investigation outcomes to be most useful. Agencies said they wanted IBAC to continue to provide such information.

Effective training to raise awareness of corruption should include content that is:

- relevant to the organisation
- tailored to the audience and its responsibilities
- created and delivered by individuals or organisations with a good understanding of corruption in the public sector
- delivered on a timely basis – as part of staff induction and as refresher training
- presented in an appropriate format, be it face-to-face or online
- supported by links to policies providing further guidance.

Fraud and corruption awareness and standards of conduct should also be promoted through regular meetings within business units in an organisation. Examples of integrity messaging initiatives agencies found successful included:

- staff newsletters promoting integrity
- organisation-wide integrity email reminders
- integrity posters or publications in public areas
- integrity website communications (intranet).

Where education and training is in place or being developed by agencies, it is important to consider their effectiveness. Staff surveys and feedback (eg through the People Matter Survey) and other reporting mechanisms can provide insight into staff awareness of fraud and corruption risks, as well as compliance with controls.[118]

4.2.1.1 Education and training

Twenty-eight agencies advised that dedicated education or training on corruption prevention is provided to their employees.[119] Most of these agencies said dedicated training is provided to all employees, and three agencies also said they provided training for contractors, suppliers and/or grant recipients.[120]

Two agencies advised only some employees are provided with training. One indicated training is provided to executives, managers and operational staff during recruit training. This agency subsequently advised it has invested in dedicated staff training in relation to its revised fraud, corruption and other losses policy, expanded training to help staff better identify and manage integrity risks across the organisation, and conducted formal training on procurement and probity requirements (including updated conflict of interest requirements for new members of procurement panels for significant projects). The other agency indicated training is provided to executives, managers, risk and compliance officers and employees working in high-risk areas. It noted dedicated training for all employees is 'to be progressively implemented during 2018'.

[118] See section 4.1.3 for further discussion on the use of surveys.

[119] Comprising nine Tier 1 agencies, 13 Tier 2 agencies and six Tier 3 agencies. Of the remaining 10 agencies (from all three tiers) who indicated dedicated training on corruption prevention is not provided, nine indicated corruption prevention and/or integrity information is integrated into other training provided to employees. Only one Tier 1 agency indicated neither dedicated training nor integrated training on corruption prevention is provided to staff.

[120] 26 agencies from all three tiers.

Training provided to all staff covers corruption and integrity-related topics such as definitions, accountabilities, prevention, detection and reporting. For example:

- One Tier 3 agency's dedicated training included the role of its corporate integrity unit, definitions of fraud and corruption, case examples, its detection program, red flags for fraud and corruption, the impact of fraud, and the protected disclosure regime.
- One Tier 2 agency's training included an introduction to fraud and corruption, risks and consequences, managing risks and responsibilities, fraud indicators and employees' responsibilities.
- One Tier 1 agency's training included topics on understanding fraud and corruption, its fraud and corruption policy framework, and reporting fraud and corruption.

Ten agencies said additional training is provided to executives and managers, risk and compliance officers, and employees working in high-risk areas. For employees working in high-risk areas, agencies advised the additional training included updates on integrity and corruption-related matters by general managers at unit meetings, probity briefings in relation to tenders, and financial management training.

Thirty agencies said corruption prevention and/or integrity is integrated into other training. Examples included all staff sessions, probity advisor presentations and training on the code of conduct, financial management, workplace obligations, procurement, finance and budget, best-practice recruitment and other operational matters.

The types of dedicated training provided to all employees by participating agencies included:

- Induction training, which was generally mandatory and conducted face-to-face.[121]
- Refresher training, which was generally mandatory but which varied in frequency between agencies,[122] including two agencies that noted refresher training was being developed or reviewed.[123]
- Online e-learning modules,[124] which were generally mandatory, as well as additional self-directed learning options available on the agency's intranet.
- Advice and, in some cases, training on changes to policy.

Other types of training identified included discussions during meetings with supervisors, information posted on the intranet, newsletters, digital screens, offline training materials for contractors, annual staff messages and internal conferences or forums.

4.2.1.2 Communication

All 38 agencies indicated they publish information for employees on expected standards of behaviour, the importance of reporting suspected corrupt conduct, and action the organisation will take in response to identified corrupt conduct.

Agencies were also asked to describe how information was disseminated or promoted. In response, agencies indicated they have promoted integrity-related messages mostly through employee training (eg induction, compulsory training or refreshers). Other methods included documents and information on intranets, emails, noticeboard messages and staff posters.

All of the agencies consider they have adequately communicated expected standards of behaviour to their employees and that the appropriate standards are in place.

[121] 13 agencies from all three tiers.

[122] 15 agencies. Frequency was not discussed in all responses, however of those that did, five agencies indicated they conducted refresher training annually, four indicated they conducted refresher training every two years, and three indicated they do so every three years.

[123] Two tier 1 agencies.

[124] Six agencies from all three tiers.

Agencies should ensure their employees are aware of expected standards of conduct, corruption risks and how to report suspected corrupt conduct. A key way to do this is by having senior managers set the tone from the top by modelling standards of conduct and encouraging an organisational culture where employees are confident about discussing potential corruption concerns.

4.2.2 Communication with the public and stakeholders

An important element of an integrity framework is employee and external stakeholder awareness of the organisation's commitment to integrity. This includes ensuring fraud and corruption-related policies, procedures, the code of conduct and other integrity initiatives (and relevant changes) are effectively communicated to all employees, suppliers, contractors, and others who have contact with the organisation. The organisation must ensure internal and external parties, including the public, are encouraged to report suspected corrupt conduct and know how to report allegations.

4.2.2.1 Suppliers

In relation to information agencies make available to suppliers:

- 30 agencies indicated they provide information regarding 'expected standards of behaviour'
- 18 said they provide information regarding 'the importance of reporting suspected corrupt conduct'
- 20 said they provide information related to 'the action the organisation will take in response to identified corrupt conduct'.

Agencies indicated the mandatory Victorian Government Supplier Code of Conduct, developed by the VGPB is the primary way they communicate integrity messages to suppliers. The code captures integrity and other expectations of suppliers and must be acknowledged by all state government suppliers. While the code provides clear guidance on expected standards of behaviour and how suppliers can report unethical behaviour or suspected corruption by other suppliers or public sector employees, it understandably does not indicate the 'action the organisation will take in response to identified corrupt conduct'. It may be beneficial for agencies to advise suppliers what the agency will do if an allegation of suspected corruption is received. Suppliers should also be assured that any reports of suspected corrupt conduct will be taken seriously by the agency.

A number of agencies also advised they provide corruption training to suppliers to reinforce those messages. For example, one Tier 2 agency provides an offline version of its fraud and corruption training materials to suppliers. Similarly, a Tier 1 agency holds 'contractor days' to communicate and share key messages about fraud and corruption awareness with its suppliers. Other initiatives included information packages for prospective suppliers and tender briefings promoting integrity, and email reminders about integrity to existing suppliers.

4.2.2.2 Funded service providers

In relation to information provided to funded service providers:

- 14 agencies said they provide information related to 'expected standards of behaviour'
- 12 indicated they provide information related to 'the importance of reporting suspected corrupt conduct'
- 12 indicated they provide information related to 'the action the organisation will take in response to identified corrupt conduct'.

Sample publications provided by agencies indicated those involved in funding third-party service providers generally included a clause relevant to the agency's integrity messages in standard funding agreements.

Like public sector agencies, funded service providers can be vulnerable to corruption risks. It would be prudent of agencies that fund third-party service providers to communicate expected standards of conduct and the importance of reporting suspected corrupt conduct.

4.2.2.3 The public

In relation to information provided to the public:

- 17 agencies indicated they publish information related to 'expected standards of behaviour'
- 17 indicated they publish information related to 'the importance of reporting suspected corrupt conduct'
- 16 indicated they publish information related to 'the action the organisation will take in response to identified corrupt conduct'.

Agencies indicated they often communicate integrity messages to the general public via websites and in publicly available annual reports. Some also noted integrity posters and other publications are promoted in public areas of the agency. Sample material provided suggests these communications focus on how to report corruption, specifically in relation to protected disclosures. However in general, agencies do not appear to have published integrity messages about the importance of reporting suspected conduct for the general public.

4.3 Information, resources and initiatives

Integrity initiatives and resources currently employed by agencies

Agencies were asked what external resources they have used to develop integrity and corruption prevention information or education materials. Thirty-two agencies provided details of the types of resources they have used, which can be grouped into seven categories:

- Policies, guidance and other Victorian government resources: 22 agencies referred to directions, guidelines, instructions, research and investigation reports, including material issued by IBAC, VPSC, Parliament of Victoria, the Victorian Ombudsman (VO), the Minister of Finance, VGPB, Victorian Managed Insurance Authority (VMIA), Victorian Auditor-General's Office (VAGO) and Victoria Police.[125] For some portfolio agencies, policies, procedures and guidance from their parent departments are often considered as well. For example, two agencies advised they used information from their parent departments to develop their own corruption prevention material and framework documentation.
- External subject matter experts: 13 agencies said they had engaged external subject matter experts to help develop corruption prevention material, conduct reviews of their fraud and corruption framework and controls, or provide advice on the development of corruption-related framework and guidance resources. These subject matter experts include legal or accounting professionals, and other experts active in fraud and corruption prevention and detection.
- External training providers and material: 10 agencies advised they had engaged external providers to develop corruption prevention training material (including electronic training resources) and/or to deliver such training to staff.

[125] 22 agencies from all three tiers.

- **Audits and reviews**: Three agencies responded that results from internal audit and other reviews of fraud and corruption controls were considered in developing corruption prevention material or education. These audits may be conducted by external parties or internally.
- **Material developed by professional associations**: Three agencies discussed the use of relevant corruption prevention material developed by professional associations including CPA Australia, the Association of Certified Fraud Examiners, and the Insurance Bureau of Australia.[126]
- **Standards**: Two agencies responded that in developing their corruption prevention materials, they referred to standards including AS8001-2008 Fraud and Corruption Control.[127]
- **Resources developed by other entities in the same sector**: One agency referred to materials developed by other entities in the same sector.[128]

Agencies were also asked to describe integrity initiatives of which they were particularly proud. Responses included initiatives that involved personalised communications and/or training, improvements to systems including automation of reporting mechanisms, promotion of integrity steering committees and focus groups, attestations and data analytics, all of which are discussed elsewhere in this report. A number of agencies also discussed initiatives involving 'experience sharing' and 'awards and other recognition' which are described on the following pages.

4.3.1.1 Awards and other recognition

Some agencies discussed awards or other ways of recognising staff who had demonstrated exceptional integrity in the workplace.

For example, one Tier 1 agency discussed the introduction of its 'Values Awards' in 2017, noting:

> *'There has been obvious evidence of pride in the recipients of these awards. Further, the general interest of other staff [regarding] the identities of the recipients further underlines interest in these awards as a vehicle for discussion regarding integrity … and strengthening morale.'*

One Tier 2 agency praised the outstanding contribution of its staff and volunteers at its annual awards event at which 'nominees from across all programs and sites are acknowledged for their extraordinary commitment to exemplifying [the agency's] key values and organisational priorities'.

Another Tier 2 agency noted it has an awards program that recognises staff who demonstrate 'community values, integrity, and excellence'. Winners of those awards are recognised on banners and have their photos displayed in common areas.

In consultations, a Tier 3 agency discussed a recent roll-out of communications related to good information security behaviours to mitigate the risk of misuse of information or material. The agency noted this roll-out was accompanied by a quiz to reinforce the message, with the winner awarded an iPad.

[126] Two Tier 2 agencies and a Tier 3 agency.

[127] Two Tier 2 agencies.

[128] A Tier 2 agency.

4.3.1.2 Experience sharing

Experience sharing was largely discussed by Tier 3 agencies, which may reflect the breadth of experience and jurisdiction of the departments, including their role in relation to regional staff and portfolio agencies.

One department noted it is proud of its regional outreach program in which staff share their stories to '[make] it real for all agency staff across the state'. Another Tier 3 agency noted two members of its executive were invited to be speakers at Institute of Public Administration Australia conferences on integrity, stating:

> *'The fact that our executive were requested to make those presentations (and agreed to do so), highlights … the appreciation for the work that has been done across the department to strengthen integrity awareness and controls over the last two years.'*

4.3.2 Development of further corruption prevention resources or activities

Agencies were also asked about other corruption prevention resources or activities they may be interested in developing. Agencies that expressed interest in developing further resources were asked about the types of content and formats that would be most useful to help with integrity and corruption prevention activities and resources.

In response, 31 agencies indicated they were interested in developing further corruption prevention resources or activities.[129]

4.3.2.1 Content

The types of issues or content the 31 agencies indicated would help them develop integrity and corruption prevention activities and resources are:

- Corruption risk controls: 16 agencies identified best-practice examples of effective controls, through case studies or real life examples. These agencies would like to understand what other organisations in the same sector have successfully implemented to prevent, detect and respond to corruption.
- Corruption risk exposures: 14 agencies indicated information related to common and/or sector-specific corruption risks would be useful. For example, one agency discussed how risk scenarios and actual cases would make corruption prevention resources 'more real and memorable' for staff, particularly if the content was specific to their sector.
- Corruption investigation findings: 14 agencies indicated information related to previous investigation findings and outcomes would be useful. For instance, one agency commented it is useful 'by way of education and awareness and as a mechanism to review fraud and corruption controls (outside of standard review schedule)'.
- Corruption framework information: 11 agencies indicated general information on corruption frameworks would be useful. Specifically, agencies would like to receive further resources about definitions of corruption, corruption risk assessment methodologies, regular corruption risk environment scans/assessments, investigation techniques, escalation protocols and 'model policies and procedures' that agencies can tailor to their organisations.

[129] This includes one agency that did not indicate whether it was interested in developing further anti-corruption resources but provided responses to subsequent questions about content and formats.

4.3.2.2 Formats

Thirty-one agencies commented on the formats that would assist with integrity and corruption prevention activities and resources. Most of these agencies noted a mix of formats would be useful. The formats have been grouped into three categories:

- Digital material: 26 agencies said digital material such as e-learning modules, podcasts, website material and media releases on IBAC investigation outcomes would be useful. This was the preferred format for agencies across the three tiers, especially for agencies that operate from a number of sites and/or have a large employee base. While IBAC has podcasts, investigation summaries, case studies and special reports on investigations available on its website, not all agencies were aware of these resources.
- Face-to-face presentations: 23 agencies noted face-to-face presentations, discussions or training would be useful including sessions with IBAC and experts. A Tier 2 agency indicated having the opportunity to meet people in similar roles face-to-face would be helpful. IBAC is aware there are a number of communities of practice operating in the Victorian public sector which provide an opportunity for participants to discuss integrity-related issues, and explore challenges and innovations. For example, IBAC convenes a community of practice for protected disclosure coordinators.
- Written material: 19 agencies said written material such as FAQs, fact sheets, reports, staff posters and case studies would be useful to their organisations. A number of agencies noted they do not have the resources to develop written policies and other integrity-related documents from scratch, and said written policies, frameworks, etc. would be helpful.

A range of information is available to help agencies create and update training and education resources. In addition to the Standard, and information and resources published by IBAC, agencies can leverage resources made available by other organisations, including the VPSC, VAGO, the Victorian Ombudsman, Victoria Police, other agencies in similar sectors, and other Australian state anti-corruption agencies.[130]

[130] For example, one Tier 1 agency's integrity framework refers to information published by the WA Corruption and Crime Commission.

5 Detection

This section considers various ways in which fraud and corruption may be identified in an organisation, noting the importance of having clear channels that encourage people to report, as well as proactively auditing to identify potential issues of concern.

According to the Standard, organisations are responsible for developing programs to detect and investigate fraud and corruption. In addition to the appointment of a targeted resource such as a fraud and corruption control officer, the Standard recommends organisations should implement systems to detect fraud and corruption. Procedures suggested by the Standard include post-transactional reviews, data mining and real-time computer system analysis to identify suspected fraudulent transactions, and analysis of management accounting reports.

The Standard advises fraud and corruption detection initiatives should be communicated to management and staff to deter those who may be motivated to engage in corrupt conduct.

Policies

Dedicated detection programs play a critical role in mitigating the risk of corrupt conduct and the associated risk to an agency's financial and reputational wellbeing. A general policy statement in an appropriate document (eg fraud and corruption control framework), which puts staff, suppliers and the public on notice that the agency has a detection program, serves as a deterrent and a means of promoting awareness of relevant reporting channels. A general statement of this kind was missing from the framework documentation provided by agencies across all three tiers. Instead, those documents tended to focus on preventative measures.

Several agencies demonstrated strong detection measures using data analytics. This is discussed below.

5.1 Identification of suspected corrupt conduct

In the 2014 review, agencies reported that corruption and misconduct was detected in three main ways: detection processes (such as audits), reports received from employees, and reports from external parties. The most common ways for investigations to commence was because of complaints made by members of the public, followed by complaints from managers and colleagues.

In this review reporting from managers and colleagues were identified as the key ways in which suspected corrupt conduct had been identified. During consultations, a number of agencies also advised they had developed fraud and corruption detection programs with advanced data analytics and data mining capabilities which help identify and respond to suspected fraud and corruption.

One size does not fit all when it comes to detection programs. Detection programs should be tailored to each agency, considering the agency's size and resources, operations, system capabilities, data quantity and quality, risk profile and effectiveness of certain controls. Agencies should consider enhancing record keeping and system capability as well as developing, documenting and embedding fraud and corruption detection programs to minimise losses from corrupt or fraudulent conduct. Detection programs could include independent reviews of transactions after they have been processed, data mining, real-time system analysis, and analysis of management accounting reports. As systems mature, so too can data analytics capabilities.

Although agencies reported receiving and responding to reports of suspected corrupt conduct from the general public and/or external parties, in general, agencies have not published messages around 'the importance of reporting suspected conduct' to the general public.[131] There is clearly value in agencies encouraging external parties, including the general public, to report suspected corrupt conduct, including by communicating how they can report suspected corrupt conduct.

This review sought to understand whether any suspected corrupt conduct had been identified in the participating agencies in the three year period from 1 January 2015 to 31 December 2017, and if so, how it was identified. Twenty-three agencies indicated suspected corrupt conduct had been identified during that period, selecting at least one of the five methods of identification suggested in the survey. Overall:

- 'Work colleagues', 'supervisors or managers', and 'a member of the public or a stakeholder' were each selected by 17 agencies as a method by which suspected corrupt conduct had been identified. This comprised:
  - seven agencies that ranked 'work colleagues' as the primary method of identification[132]
  - seven agencies that identified 'supervisors or managers' as the primary method of identification[133]
  - three agencies that identified 'a member of the public or a stakeholder' as the primary method of identification.
- 'Protected disclosure procedures' were selected by 12 agencies as a method by which suspected corrupt conduct had been identified, however only four agencies ranked it as the primary method of identification.
- 'Compliance or monitoring systems' were selected by 13 agencies as a method by which suspected corrupt conduct had been identified, however only two agencies ranked it as the primary method of identification.

These responses suggest that in agencies where suspected corrupt conduct has been identified, reliance is placed on employees for identification or reporting. However, the consultations with agencies highlighted some other innovative approaches and an increased awareness of the value of data analytics.

Data analytics and data mining are generally performed by teams using structured data that can be readily analysed. These teams may include, but are not limited to, finance, IT, forensics, internal audit and procurement. Analytics can be performed as ongoing regular monitoring exercises and/or as required when potential issues are identified. In some circumstances, ad hoc analytics may eventually become ongoing exercises if systemic issues are identified that require continued monitoring.

When internal resources and capabilities are limited, agencies could consider leveraging external subject matter expertise to undertake the initial data analytics set-up. Agencies could also consider ongoing analytics in relation to specific key risks, leveraging fraud and corruption risk assessments. However, once issues are identified, agencies must follow through and ensure appropriate further enquiries and action are undertaken.

While some data analysis may be sophisticated, there are some simple checks that most, if not all, agencies could consider, as illustrated in the case studies on the following page.

[131] See section 4.2.2 for discussion of communication with the public and stakeholders including integrity messaging initiatives used by agencies.

[132] Agencies were asked to indicate the most common ways in which suspected corrupt conduct was identified by numbering options from 1 to 5 where relevant.

[133] This includes one agency that ranked 'supervisors or managers' as '2', but did not select any other methods of identification.

DETECTION OF SUSPECTED CORRUPTION USING DATA ANALYTICS

Case study 16

One Tier 3 agency maintains an in-house forensic laboratory, with two employees designated to support efforts to detect possible fraud and corruption. The agency advised the laboratory performs regular background forensic analysis of all network drives, website access, email profiles, archives, and phone/iPad data (if employees have used work computers to back up personal phones/tablets). This involves screening 500 to 700 computers a year (ie about 125 computers a quarter), of which 75 per cent are random scans. The other 25 per cent focus on devices used by employees in high-risk roles, including employees working in human resources, finance, procurement or on programs responsible for allocating public resources. Other high-risk criteria include employees with financial delegations or high leave balance.

Tests performed include screening:

- event invitations received and accepted by employees via email, and comparing the invitation to the gifts register to check compliance with the gift, benefits and hospitality policy
- potential private interests of employees and comparing to declared conflicts of interests and private interests to check the accuracy of the declaration
- employee contact lists (if the phone was backed up on an agency computer) against a list of individuals involved in organised crime
- all computer systems for general fraud and corruption risks using a word list tailored to the agency
- images to identify extreme images, including pornography.

Although details of the agency's suppliers are not screened as part of the detection program, every three years supplier data is compared to employee data to identify matching bank account information.

Each hit is reviewed, noting the process can sometimes generate false positives (eg when employees also receive funding or a grant from the same department). In the last three-year analysis, one per cent of all hits was determined to be suspected corrupt conduct and referred to IBAC.

Independent of its ongoing screening processes, the agency recently screened individuals named in the Panama Papers against a list of its employees.[134] Two false positives were ruled out after the team cross-checked individuals' dates of birth, addresses and other information. The finance team performed the same matching exercise for the agency's suppliers and examined the services provided by entities referred to in the Panama Papers.

Case study 17

Another Tier 3 agency advised that three employees work full-time on compliance reviews and conduct monthly reconciliation of corporate credit cards. Data analytics are used in this process and often detect policy breaches. The agency's finance team also uses this analytics process to check transactions related to accommodation, flowers, restaurants and duplicate payments – with a focus on expenses incurred at weekends.

Case study 18

A Tier 1 agency noted that in addition to regular audits of the financial, human resources, information technology and procurement sectors, the agency utilises a data analytics compliance monitoring system to collate, track and compare employee data and declarations. This data includes information from employee attestations and conflict of interest documents, and is compared to complaints received about employees or pending investigations. Only compliance officers and managers overseeing investigations have unlimited access to the data within this system.

[134] The Panama Papers are millions of leaked documents that detail information related to more than 200,000 offshore entities, some of which were alleged to be used for fraud and tax evasion. The documents were leaked in 2016.

5.2 Reporting channels

5.2.1 Protected disclosures

During the period of this review, the legislation concerned with protecting people who make disclosures about improper conduct in Victorian public sector agencies was the Protected Disclosure Act 2012. A new 'public interest disclosure' (PID) scheme will replace the protected disclosure scheme from 1 January 2020. The new legislation makes some changes to the entities that can receive PIDs. For the purposes of this report, we refer to 'protected disclosures'.

The 2014 review noted that while a number of agencies had developed or were developing protected disclosure requirements, most reporting systems or complaints mechanisms related only to suspected fraud rather than suspected corruption.

In October 2016, IBAC published guidelines for making and handling protected disclosures, and guidelines for protected disclosure management, which provide guidance to protected disclosure coordinators, public sector agencies, individuals wishing to make disclosures, and entities responsible for investigating disclosures.[135]

In this 2019 review, documentation provided by most agencies reflected these documents, and these policies appear well embedded. This is to be expected given the protected disclosure regime has now been in place for more than five years.

Mandatory reporting provisions were introduced in December 2016, requiring relevant principal officers of public sector agencies to notify IBAC of suspected corrupt conduct they reasonably believe has occurred or is occurring.

Under the Protected Disclosure Act, not all public sector agencies can receive protected disclosures.

Under that legislation, Victorian departments, administrative offices, councils and the VPSC can receive disclosures about the conduct of their own employees.[136] Along with the other investigating entities (VO, Victoria Police and the Victorian Inspectorate) IBAC can receive protected disclosures about these agencies, as well as receiving protected disclosures relating to agencies that cannot receive such disclosures directly.

The 38 participating agencies included nine agencies that could receive protected disclosures and 29 agencies that could not under the Protected Disclosure Act. In response to the survey, the nine agencies that could receive protected disclosures (the seven Tier 3 departments and two Tier 1 agencies) all correctly responded that they were able to receive protected disclosures.

Of the 29 agencies that could not receive protected disclosures, seven incorrectly stated they could receive protected disclosures in their survey response. Four of these agencies provided documentation that was inconsistent with their survey response (ie their policies correctly stated protected disclosures must be made directly to IBAC). The policies of the other three agencies inaccurately stated a protected disclosure about the agency could be made directly to the agency. However, all three agencies subsequently advised their protected disclosure policies had been corrected to state that disclosures should be made directly to IBAC.

[135] See: www.ibac.vic.gov.au/publications-and-resources/article/guidelines-for-making-and-handling-protected-disclosures and www.ibac.vic.gov.au/publications-and-resources/article/guidelines-for-protected-disclosure-welfare-management.

[136] For a list of agencies able to receive protected disclosures, see www.ibac.vic.gov.au/docs/default-source/education-resources/fact-sheet---what-is-a-protected-disclosure.pdf

These responses suggest some agencies may not have a clear understanding of what should be reported internally, and what needs to be reported to IBAC. However, most of the 10 agencies involved in the consultations advised they felt informed and prepared to handle protected disclosures, irrespective of whether they were authorised to receive them. Most agencies also confirmed that training is provided to appropriate staff (eg protected disclosure coordinators, human resource officers). For example, one Tier 3 agency offers protected disclosure notification training for its employees which links to external resources and information. Many organisations confirmed they primarily use IBAC resources for education on protected disclosure handling.

A number of agencies noted they had sought guidance from IBAC when preparing their protected disclosure and other reporting-related policies. For instance, during consultation, one Tier 2 agency stated IBAC is responsive in answering any questions related to the protected disclosure process, and the agency usually contacts IBAC directly if it encounters a question that cannot be answered using IBAC's publicly available materials.

IBAC RESOURCES

IBAC has a number of useful resources on its website that provide information to the Victorian public sector and the community on reporting corruption. These include:

- *Public sector corruption hurts all Victorians*[137]
- *Reporting corruption and misconduct*[138]
- *What is a protected disclosure?*[139]

Performance of responsibilities under the Protected Disclosure Act

Agencies that can receive protected disclosures are required to have procedures in place to facilitate the making of disclosures, and to receive and manage disclosures (including the making of notifications to IBAC). This may include appointing a protected disclosure coordinator to whom employees or community members can report.

The nine participating agencies able to receive disclosures under the Protected Disclosure Act generally indicated the role of protected disclosure coordinator is a function performed in addition to other duties by an employee at the executive level in either human resources, risk, legal, finance or governance areas.

Participating agencies that could not receive protected disclosures generally indicated they advise individuals to make a disclosure to IBAC directly. For instance, one Tier 1 agency has published guidance on its website directing people to contact IBAC if they wish to make a disclosure about the agency or its staff, and sets out the agency's procedures for managing disclosures in a way that will protect the discloser from reprisal and provide welfare management.

5.2.2 Other internal reporting

Most agencies across all three tiers indicated staff are encouraged to report suspected fraud and corrupt conduct to a senior officer. Twenty-one agencies indicated internal reporting channels included reports to a supervisor, manager or executive, while 16 indicated they have a dedicated individual or team to accept reports. Other internal reporting channels included external complaint hotlines,[140] online reporting systems,[141] and protected disclosure coordinators.[142]

[137] IBAC information sheet, *Public sector corruption hurts all Victorians*, August 2017.

[138] IBAC fact sheet, Reporting corruption and misconduct, July 2016.

[139] IBAC fact sheet, *What is a protected disclosure?* February 2018.

[140] Six agencies from all three tiers.

[141] Three agencies from all three tiers.

[142] Six agencies from all three tiers.

Several agencies discussed to whom their staff could report suspected corrupt conduct more broadly, identifying external channels such as IBAC,[143] the Victorian Ombudsman,[144] and Victoria Police.[145]

Agencies were also asked to describe the measures in place to ensure protected disclosure and other internal reporting systems were operating effectively. Thirty-one agencies provided a response to this question, primarily citing board or committee oversight as an assurance mechanism.[146] Other measures identified as helping to measure the effectiveness of reporting mechanisms included audit activities, reviews of policies and procedures, and surveys (including the People Matter survey, other 'employee surveys' and exit surveys).[147]

USING SURVEYS TO MEASURE THE EFFECTIVENESS OF REPORTING MECHANISMS

Case study 19

In developing its training and communication program for employees, a Tier 1 agency advised it reviews feedback obtained from the People Matter survey to ensure its training and communication program responds to real life examples of integrity issues faced within the organisation. This makes the training more relatable and effective.

In addition to encouraging participation in the People Matter survey, a Tier 2 agency has developed its own survey to test employee knowledge and understanding of integrity messages communicated by the organisation, including reporting options.

Access to reporting channels

To ensure there are effective channels for reporting suspected corrupt conduct within their organisations, agencies should consider encouraging reports from a wide range of sources (ie not just employees) including reports from contractors, service providers, suppliers, former employees, members of the community and customers/clients.

Agencies should also ensure reporting channels are easily accessible to the different groups of people who may make a disclosure. Communication of reporting channels should be clear, concise and indicate:

- how confidentiality of reports will be maintained
- what will happen after a report is received
- protections in place for the disclosers, where applicable.

Triage of reports

Agencies should have a proper triage process in place to ensure:

- reports received are documented properly
- subject matter experts are involved when necessary
- conflicts of interest are avoided when allocating investigations of the disclosures
- there is proper oversight and review during the management of the disclosure (eg integrity steering committees or panels)
- if appropriate, matters are referred to relevant agencies.

[143] Ten agencies from all three tiers.

[144] Three agencies from all three tiers.

[145] Three agencies from all three tiers.

[146] 17 agencies from all three tiers.

[147] Each discussed by seven agencies.

To further increase accountability, smaller agencies could ensure reporting avenues include positions that are separated from the CEO to provide an escalation mechanism and an alternative means of reporting matters that relate to the CEO. For instance, the survey responses of one Tier 2 agency suggest notifications of integrity concerns are currently communicated directly to the CEO (via a feedback form on the agency's website), which does not appear to provide any escalation or alternative internal reporting avenue, particularly if a concern related to the CEO.

However, the agency subsequently advised it has policy documents that outline avenues for staff to report suspected fraud and corruption including a process to report to the Board Chair where the CEO may be suspected of being involved, as well as a reporting process if the Board Chair is implicated.

The agency's policies also document protected disclosure processes (which must be made directly to IBAC), and reports to managers, including escalation processes if the manager fails to respond appropriately and quickly. Regular reminders are circulated to staff to promote awareness of their responsibility to report any concerns. One example of this is a fortnightly message to staff from the CEO encouraging employees to speak up if something is not right.

5.3 Audits

Audits can play a key role in detecting fraud and corruption. Audit outcomes are also a key indicator of whether controls to prevent, detect and respond to fraud and corruption risks are operating effectively.

The Standard recommends organisations that undergo financial audits should be familiar with the role and responsibilities of the auditor in detecting fraud and corruption. Audit committees and senior leaders should understand audit procedures that are specific to detecting discrepancies in the entity's financial statements that may be due to fraud or corruption.

Audit standards state an auditor is responsible for obtaining reasonable assurance that the financial report as a whole is free from material misstatement, whether caused by fraud or error. The Standard states, prior to audit, organisations should:

- emphasise to the auditor the importance the entity places on fraud detection as part of the audit
- offer all documentation the auditor may require to enable a more comprehensive review
- consider fraud risk factors set out in the Standard.

Internal audits are an important way of identifying indicators of fraud and corruption relevant to specific organisations, and to detect fraud and corruption. Fraud and corruption reviews should be considered during planning for agencies' internal audit programs. Audit programs designed to test operational processes should include testing of controls which aim to mitigate fraud and corruption risks within business units or processes. For example, when developing the internal audit scope to test procurement management, it is important for agencies to consider potential fraud and corruption risks associated with procurement, and to include procedures to test related controls, such as management of conflicts of interest.

Auditing exercises are of limited value if identified weaknesses are not addressed, specific breaches are not investigated, or proposed improvements are not implemented or tested. Agencies should ensure results from internal and external audits are centrally documented and monitored, and recommendations are transferred to actionable items with clear responsibilities and completion dates assigned. Relevant managers should monitor the progress of actions, and results should again be reviewed and certified. Future audits conducted in the same area should refer to previous audit results and recommendations and validate whether changes or enhancements, have been made. The results should also be considered during future fraud and corruption risk assessments conducted by the agency.

5.3.1 Policies

Documentation provided by Tier 3 departments included evidence of external audit reporting procedures focused on fraud and corruption controls. Such materials were provided in lieu of dedicated fraud and corruption detection programs. Certain agencies supported VAGO in its audits by sharing their fraud and corruption risk assessments and results from any investigations conducted into suspected incidents of fraud and corruption.

Documentation provided by Tier 1 and Tier 2 agencies was generally silent on the use of audits to control corruption risks, noting only that VAGO performs audits of financial statements and compliance with accounting standards.

5.3.2 Practices

The review indicated compliance monitoring, including audits, is a key way suspected corrupt conduct had been identified. Some agencies also discussed the role of VAGO in identifying suspected fraud and corruption. For example, one agency noted:

> *'… whilst VAGO are not responsible for preventing and detecting fraud, they are required to consider the risk of material misstatement due to fraud or error when performing their risk assessments. Under the Audit Act 1994, VAGO are required to notify IBAC where they become aware of any matters that appear to involve corrupt conduct.'*

External providers with subject matter expertise often conduct agencies' internal audits, and many agencies discussed having internal audit programs to review and identify opportunities to strengthen fraud and corruption frameworks and controls. It was also noted that operational areas at higher risk of fraud and corruption (procurement, cash handling, information security and fund or grant management) were often subject to more frequent and stringent internal audits. The results of internal and external audits are often considered during fraud and corruption risk assessment processes, and accountability is usually assigned to individuals to ensure audit issues are addressed and recommendations implemented.

6 Conclusion

The Victorian public sector delivers goods and services that impact many aspects of our lives. The Victorian community rightly expects state government employees to conduct themselves with integrity.

It is important state government agencies have strong integrity frameworks comprising policies and procedures, processes, systems and controls to promote integrity and help prevent and detect corrupt conduct. Integrity frameworks should also be regularly reviewed to identify areas for enhancement, and to consider insights from other agencies and the broader public sector.

This review of integrity frameworks in 38 state government agencies indicated shifts in agencies' perceptions of corruption risks, and development of their integrity framework and controls since a similar review was conducted in 2014, including:

- corruption risks listed in the review survey are now definitely on the radar of most participating agencies
- agencies generally understand the definition of corruption, what corrupt behaviour looks like, and where it should be reported
- senior leadership commitment to integrity measures is evidenced in policies and procedures, and in practice with a number of agencies indicating they have staff or committees responsible for considering and promoting integrity measures
- most participating agencies have developed and/or are providing dedicated corruption and integrity training to internal and/or external stakeholders
- awareness of the potential of data mining and data analysis has increased, based on comments during the consultations with the 10 agencies, all of which said they had introduced data analytics to detect potential corrupt conduct or were considering it.

Mechanisms for reporting suspected fraud and corruption have matured, evidenced by the majority of participating agencies having documented policies and procedures, and demonstrating a better understanding of protected disclosures. It is critical employees are encouraged to report suspected corrupt conduct and understand the protections available to them if they report.

The review also revealed ways in which agencies can enhance their integrity frameworks:

- agencies should consider including integrity-related behaviours in employee performance plans, as a stand-alone item or as part of organisational values against which employees' behaviours are assessed
- requiring conflict of interest declarations to be made electronically to reduce the chance of mistakes or omissions when data is transferred from paper format, and to improve central oversight
- a centralised electronic repository of all declarations facilitates the identification of potential conflicts with other parties
- training and communication about integrity should be tailored to specific roles and presented in interactive formats, to significantly improve staff engagement, awareness, and retention of integrity messages
- appropriate levels of screening should be considered for shortlisted candidates for positions, as well as re-screening for employees moving to a new position, particularly those considered 'high risk' in terms of potential exposure to fraud and corruption
- due diligence should be conducted before engaging suppliers. Background checks, supported by declarations from a prospective supplier, can help an agency identify corruption and other risks. Due diligence should include the validation of information collected from the supplier, and through third party, independent sources.

All state government agencies are encouraged to consider this report to identify ways in which they can continue to strengthen their own integrity frameworks, to improve their capacity to prevent corrupt conduct.

IBAC thanks the 38 state government agencies for their involvement in this review.

ibac independent broad-based anti-corruption commission
Victoria

Level 1, North Tower
459 Collins Street, Melbourne Victoria 3000
GPO Box 24234 Melbourne Victoria 3000
Phone 1300 735 135 | Fax (03) 8635 6444

www.ibac.vic.gov.au