

# *Fighting fraud in the public sector*

*The government and  
public sector extract  
from PwC's Global  
Economic Crime Survey*

*June 2011*



**pwc**

*What would you like to grow?*

---

# Contents

**03**

*About  
the survey*

**04**

*Key findings*

**05**

*Economic crime  
in the Australian  
public sector*

**08**

*The profile  
of a fraudster*

**12**

*Prevent, detect,  
respond*

**19**

*What's on the  
fraud horizon?*

**20**

*Conclusion*

**21**

*Methodology*

**25**

*PwC Forensic  
Services:  
An Overview*

# About the survey

Welcome to the government and public sector extract from PwC's latest Global Economic Crime Survey and observations from recent fraud surveys published by Australian Auditors-General<sup>1</sup> and the Australian Institute of Criminology (AIC).<sup>2</sup>

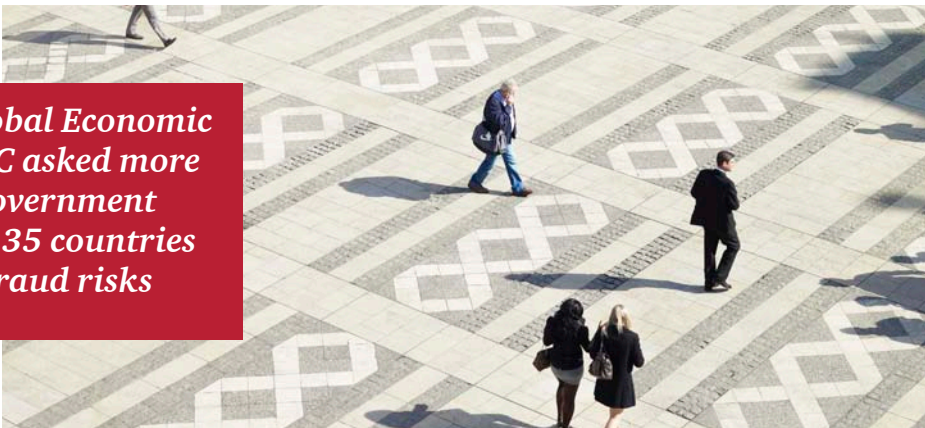
*This extract comes against a background of a relatively robust Australian economy, but continuing global political and economic instability. Despite the general overall health of the economy, the public sector is under pressure from planned and expected job cuts at the state government level.*

*To compile the PwC Global Economic Crime Survey, we asked more than 170 senior representatives of government and state-owned enterprises in 35 countries about fraud and fraud risks. For further details of the survey demographics, see the 'Methodology' section on page 21.*

*The survey scrutinised fraud and associated integrity risks during a period of considerable economic turmoil. It investigated the root causes of fraud and its effects on organisations worldwide.*

*We would like to thank the Australian public sector respondents who participated in the survey and the Auditors-General for making their findings publicly available. We hope the insights included in this survey will help government and state-based organisations combat fraud and other economic crimes.*

**Cassandra Michie**  
Partner  
PwC



**To compile the Global Economic Crime Survey, PwC asked more than 170 senior government representatives in 35 countries about fraud and fraud risks**

- <sup>1</sup> ANAO Audit Report No. 42 2009–10 Fraud Control in Australian Government Agencies (ANAO's Fraud Control Report); NSW Auditor-General's Report to Parliament 2010 Volume Two Fraud Control Arrangements in Large Government Agencies and Universities (Ten Elements of Fraud Control). (NSW Auditor-General's Fraud Control Report). The remaining statistics are based on the PwC Global Economic Crime Survey 2009.
- <sup>2</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011.

# Key findings

## Six important findings

*In Australia, state and federal government departments are variously expanding and contracting. Expansion represents a fraud risk where fraudsters are attracted to new programs and projects, and take advantage of situations where controls and risk assessments are still being formulated. Contraction also represents a risk, as cutbacks reduce the integrity of controls, especially segregation of duties, and the resources to monitor transactions such as internal auditing.*

1. Government and state-owned enterprises on average experienced a higher incidence of fraud than listed private entities. More than one-third (37%) of respondents from government and state-owned enterprises said they experienced economic crime in the previous 12 months. This is consistent with the AIC 's findings of 39% of Australian Commonwealth Agencies having experienced fraud.<sup>3</sup> Senior executives need to be aware of their organisation's risk profile.
2. Government and state-owned enterprises reported that 69% of the fraud they suffered related to the misappropriation of assets and this category of fraud needs to be a focus for senior executives.
3. Staff members perpetrated more than half (57%) of fraud reported by government and state-owned enterprises, compared to only 25% for financial services organisations. Senior executives in government organisations need to be aware of 'the enemy within'.
4. Senior staff are more likely to commit fraud in government and state-owned enterprises than in any other industry.
5. More than one-third (39%) of New South Wales government agencies told the state Auditor-General their fraud risk assessments were not effective and senior executives need to understand why this is the case in their organisation.<sup>4</sup>
6. Government appears to be lenient on perpetrators of fraud, with only 51% of internal fraudsters at government and state-owned enterprises being

dismissed from their jobs. This compares to 60% across all industries. Senior executives in government organisations need to be aware of the message this sends to their organisation and the role they play in setting the tone from the top.

## The PwC perspective

From our experience, Australian government and state-owned enterprises are most susceptible to fraud when:

- they have large, demand-driven spending commitments driven by policy, which do not allocate enough time and resources to assess risk or implement controls to detect, investigate and mitigate fraud
- power is centralised unduly; for example, when a single individual has the power to make decisions on procurement, contracting and approval
- standard contracting procedures are bypassed using the justification of 'addressing urgent business needs'. This temporary approach may then be extended to avoid the checks and balances of procurement policies
- policies and rules to minimise fraud and corruption are not applied with the same rigour in remote operations as in the head office
- an excessive focus on outcomes can result in increased pressure to improperly modify results, a loss of accountability and poor maintenance of associated business records
- when fraud is suspected, if processes are flawed and associated records are inadequate, this may lead to insufficient evidence being available to mount a successful investigation or prosecution. It may also result in the agency concerned being unable to instigate civil recovery action
- as leaders within their organisation, senior executives have a critical role to play in controlling fraud in the government sector. It is important that they set the right tone from the top and ensure that they and the staff they lead understand their particular fraud risks and profile and that these risks are on the radar and treated seriously. The new Commonwealth Fraud Control Guidelines issued in March 2011 are definitely a step in the right direction with more prescriptive requirements on fraud risk assessments and fraud control planning.

<sup>3</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, page 7

<sup>4</sup> NSW Auditor-General's Fraud Control Report, page 6

# Economic crime in the Australian public sector

While Australia may not have been affected to the same degree in the recent economic downturn as other countries, many state governments have announced a reduction in public sector reduction programs. In addition, we understand government departments are tightening performance metrics, which may add to workers' concerns over career progression.

## Understanding the risks

### Moving beyond compliance

The PwC *Global Economic Crime Survey* revealed that workers' fear of redundancy and organisations' propensity to set ever more difficult performance targets, together with a continuous stream of new policies of spending programs, exacerbated the risk of economic crime.

At PwC, we believe that government and state-owned enterprises therefore need to evaluate their fraud risks and manage them effectively.

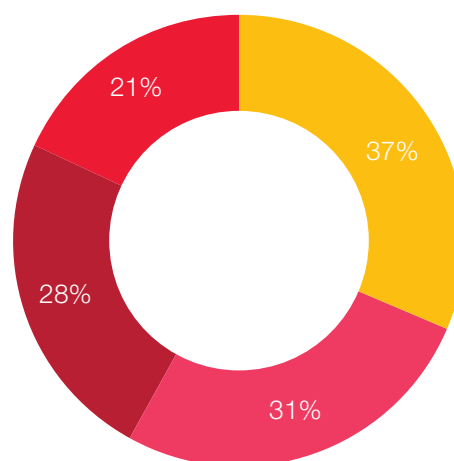
The recent update to the Commonwealth Fraud Control Guidelines of 2011 bring them in line with Australian Standard 8001 *Fraud and Corruption Control*, and provide a more comprehensive fraud risk framework. Highlights include:

- a requirement to reassess fraud risks with any change in organisation structure, or any major new or changed policies
- specifically assigning accountability of fraud control plans to chief executive officers
- a revised emphasis on fraud training and awareness programs
- a requirement to provide an appropriate channel for reporting fraud.

### The extent of economic crime in the previous 12 months

More than one-third (37%) of respondents reported in the PwC *Global Economic Crime Survey* that their government or state-owned enterprise had experienced economic crime in the previous 12 months; this is consistent with the findings of the AIC for 2008/2009 at 39%. This compares to 31% for listed companies and 28% for the private sector.

Figure 1: Percentage of organisations reporting fraud in the previous 12 months



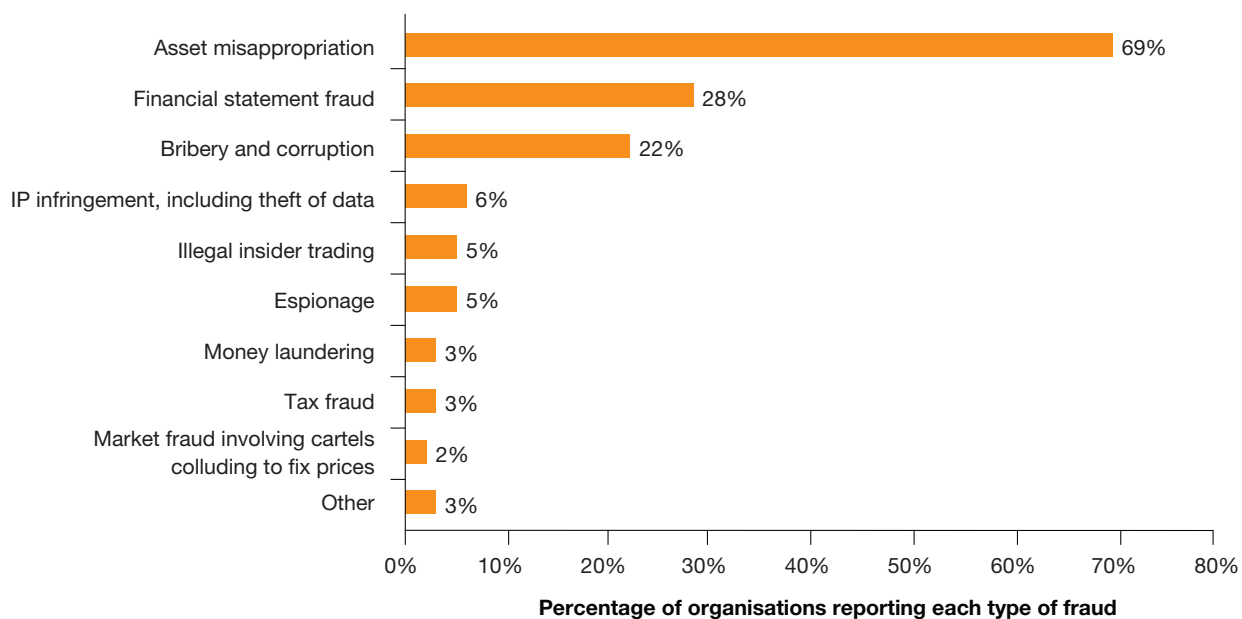
- Government and state-owned enterprises
- Listed companies
- Private sector
- Others

### What kind of fraud is occurring?

Economic crime takes many different forms. Figure 2 shows the types of crime suffered by those government and state-owned enterprise respondents that reported experiencing economic crime in the previous 12 months.

Over two-thirds (69%) of those reporting economic crime suffered asset misappropriation. This type of fraud is the most prevalent economic crime and covers a variety of misdemeanours. While asset misappropriation is the hardest form of economic crime to prevent, we believe it is the easiest to detect as the assets or funds can usually be traced or observed moving in or out of the organisation.

**Figure 2: Types of economic crime experienced by government and state-owned enterprises that reported experiencing fraud in the past 12 months**



The New South Wales Auditor-General’s survey stated that the most common types of fraud perpetrated by employees were:

- theft, including cash, consumables and intangible assets
- procurement fraud, such as false invoicing and credit card misuse
- payroll fraud
- fraudulent expenditure claims.<sup>5</sup>

The Australian National Audit Office (ANAO) 2009 fraud survey includes in its list of fraudulent activities:

- unauthorised or inappropriate use of information technology
- the unauthorised access and release of information
- the forgery or falsification of records
- identity fraud
- fraud in the way government conducts business, such as outsourcing of service delivery to external service providers, the introduction of new policy initiatives and programs, introduction of internet-based transactions and electronic information exchange.

Fraud is not confined to misappropriation. Accounting fraud encompasses a variety of actions, including accounting or reporting manipulations and accounts for 28% of economic crime involving government.

Key Performance Indicators (KPIs) have become an important measure of success for many government agencies. We are also seeing a far greater emphasis within the public sector on reporting, with funding often tied to the outcomes. As KPIs become more refined and harder to achieve, government and public sector employees face increased incentives, and pressure, to mis-state records or focus on meeting targets rather than achieving outcomes. As a result, we have seen an increase in the number of investigations of statistical reporting – for example, a number of inquiries here and overseas have been conducted in relation to patient waiting list data and connection to funding.

### Case study

*The Independent Commission against Corruption has undertaken a number of investigations relating to the misappropriation of funds. These investigations have focused on employees:*

- using false receipts to claim travel and accommodation allowances
- removing and selling inventory
- receiving kickbacks for referring contract work to past employees
- directing contracts to companies they had established.

<sup>5</sup> NSW Auditor-General’s Fraud Control Report, page 4

## Bribery and corruption

Worldwide, 22% of respondents from government and state-owned enterprises that experienced economic crime reported cases of bribery and corruption in the last 12 months. The AIC reported that in the 2008/09 year there were 75 incidents of bribery of an employee.<sup>6</sup>

However, in recent years there has been a global change in attitudes towards bribery and corruption, resulting in increased regulation. Bribery and corruption is not regarded or accepted as a 'cost of doing business', and is a form of economic crime that adversely impacts both the individuals and entities involved and society as a whole.

This trend is likely to continue as more jurisdictions strengthen anti-corruption legislation and enforcement actions in response to global pressures.

However, counterbalancing tougher enforcement are the growing financial pressures on companies doing business with government and the public sector. As those pressures increase, these companies may be tempted to use illicit means to secure contracts, and government officials may increasingly be presented with bribes or other incentives to steer business in a certain direction.



### **International efforts to curb bribery and corruption**

*Countries around the world are tightening legislation in relation to bribery and corruption by:*

- criminalising acts of corruption, as signatories to international anti-corruption frameworks such as the United Nations Convention Against Corruption and the Organisation for Economic Cooperation and Development Anti-bribery Convention*
- investigating and prosecuting individual executives, not just organisations*
- collaborating with other governments to prevent transnational corruption*
- creating anti-corruption bodies such as a supreme audit board, and specialised enforcement agencies such as the NSW Independent Commission Against Corruption and the Victorian Integrity and Anti-Corruption Commission*
- creating effective legal systems for seizing, freezing and confiscating the assets or proceeds of a crime*
- developing transparency in government operations and public procurement, and establishing enforceable codes of conduct for government officials*
- imposing significant fines on companies, in two recent cases in the US, companies have agreed to pay fines of over USD\$1.5 billion for breach of the Foreign Corrupt Practices Act.*

<sup>6</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, page 24

# The profile of a fraudster

## Who is committing fraud?

Understanding who is likely to commit fraud and the circumstances under which individuals may 'cross the line' can help organisations focus their anti-fraud policies in the right areas. For example, opportunists could take the chance to enrich themselves from programs that are in the early stages of development and have limited controls.

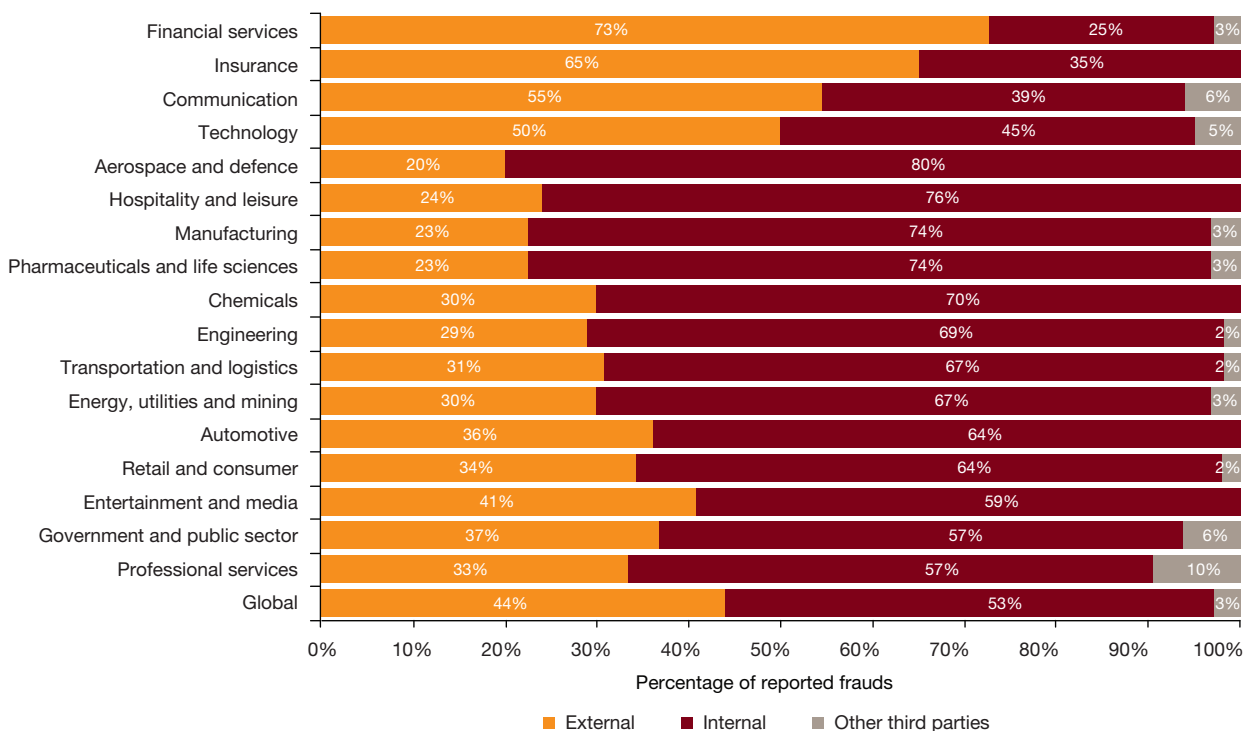
Equally, senior managers under intense pressure to meet high targets may resort to unethical means to achieve their goals.

Within government and state-owned enterprises around the world, fraud seems to be more of an internal than an external phenomenon. Based on the PwC *Global Economic Crime Survey*, government entities around the globe that suffered from economic crime reported that 57% of perpetrators were internal while only 37% were external. This internal threat is significantly higher in the public sector than in most other sectors. The AIC findings are not as stark, 32% of agencies experienced internal fraud compared to 30% external. The threat of internal fraud is still great.

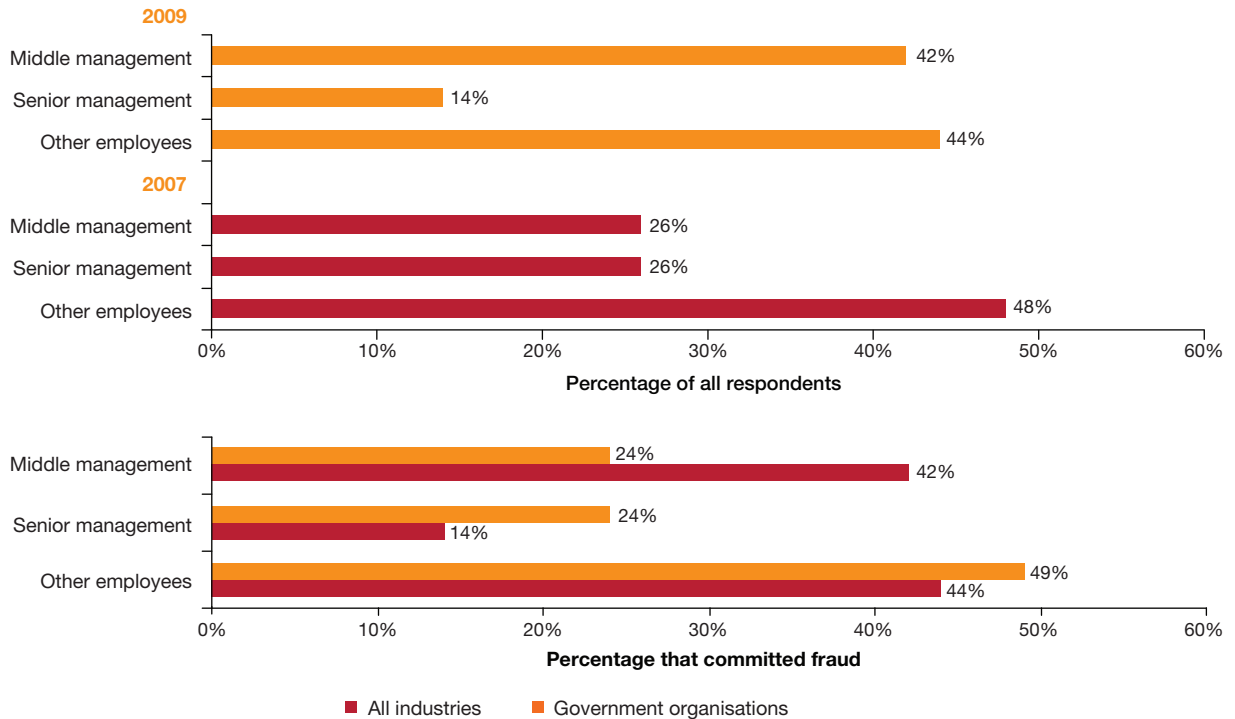
In our experience there is no such thing as a "typical internal fraud perpetrator". Equally anecdotal evidence points to the most successful offenders being well-regarded by their peers and it often comes as a shock to those around them when they are eventually caught. It is the perpetrator's 'likeability' that plays a strong role in assisting them to go undetected because those around them do not attribute inappropriate motives to their actions.

The problem with developing a typical offender profile is that it can blind managers to the significant proportion of perpetrators who do not fit the profile. Conversely, innocent persons in the workplace who fit the profile may be subjected to inappropriate focus without justification.

According to the PwC *Global Economic Crime Survey*, the share of economic crime committed by middle management across all sectors rose from 26% in 2007 to 42% in 2009.



**Figure 4: Profile of internal fraudsters**



In contrast, within government and state-owned enterprises, the number of crimes committed by middle management has remained steady at 24%. In the government sector, junior managers are most likely to commit fraud (49%) but senior executives committed 24% of economic crime, significantly higher than the all-industries figure of 14%.

### Why do people commit fraud?

Fraud investigators often point to three common factors when fraud occurs (the ‘fraud triangle’). First, perpetrators of fraud need an *incentive* or *pressure* to engage in misconduct. Second, there must be an *opportunity* to commit fraud, and third, perpetrators are often able to rationalise or justify their actions.

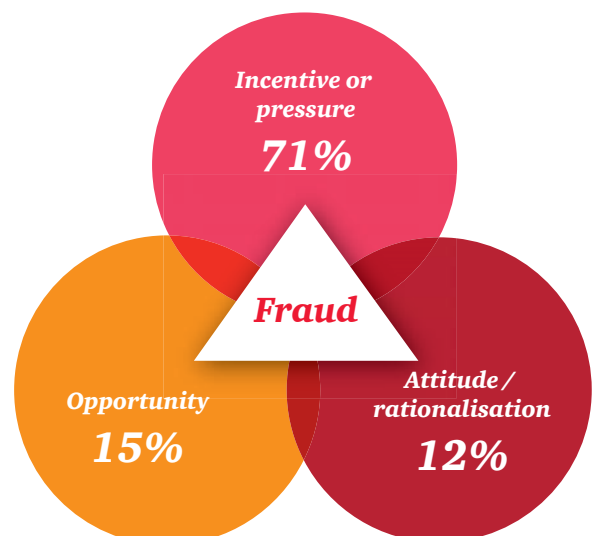
The PwC *Global Economic Survey* found that:

- 71% of respondents attributed greater risk of fraud to increased incentives or pressures
- 15% claimed “more opportunities” as the most likely reason for greater risk of fraud
- 12% believed that people’s ability to rationalise was the main factor contributing to greater risk of fraud.

What’s behind these perceptions? In the public sector, the survey found that the most commonly reported factor motivating people to commit fraud was fear of losing their jobs.

Globally, this pressure is set to increase with the expected cuts across the public sector in the next 12 to 18 months. While arguably this pressure is not as great in Australia with its relatively stable government workforce, staff can still be motivated to commit fraud by the loss of promotion or the lack of job opportunities.

**Figure 5: The fraud triangle – Why do people commit fraud?**

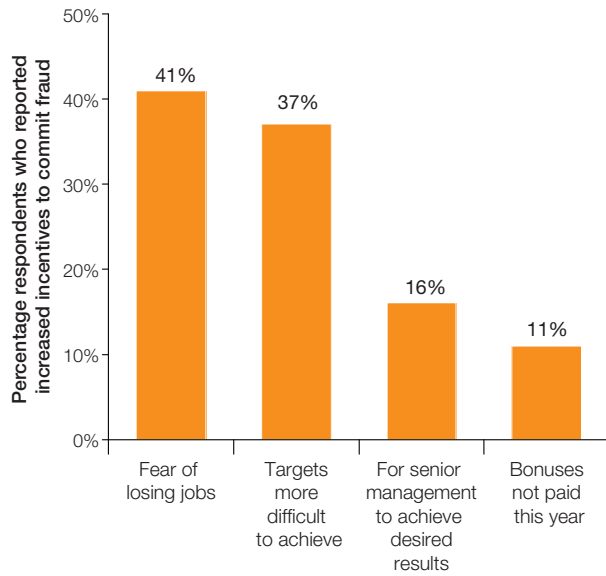


Public sector cuts also result in additional work pressures on those who remain. This often leads to reductions in accountability as checks and balances fall by the way-side because fewer people are being required to do more work. The result can be increases in both internal and external fraud because fewer people are available to monitor controls.

Many respondents were concerned that government departments were looking to cut the cost of non-essential services. In the private sector internal audit or quality reviews are often targeted for cut back. Coupled with the existence of some very large government programs, such potential cuts present a strong fraud opportunity.

We believe it is important that organisations monitor performance closely and correlate sources of information to identify when staff might feel under particular pressure.

**Figure 6: Factors given by respondents from government and state-owned enterprises as contributing to increased incentives to commit fraud**



**65%**

*believe that IT controls are weakening, making organisations more vulnerable to external penetration*



## Reduced control?

Of those government and state-owned enterprise respondents who perceived greater opportunities to commit fraud in the current environment, 55% believed that staff reductions meant fewer resources were used to support internal controls.

Financial difficulties force organisations to reduce costs and explore possible efficiencies. Any resulting staff reductions can lead to reduced segregation of duties and less monitoring of suspicious transactions and activities. This in turn weakens the internal control environment and can produce more opportunities for staff to commit fraud.

The NSW Auditor-General's report echoed this view: "Fraud risks in the New South Wales public sector have been further heightened by the rationalisation of 'back office' activities. If not planned well, gaps in vital internal controls can occur. Key controls such as the segregation of duties need to be maintained, particularly in finance areas. The 'back office' is where many of the fraud controls need to be."<sup>7</sup>

It is therefore important that organisations consider how they employ their resources and ensure they make sufficient investment in detection tools, such as data analytics, that can help fight fraud. This was highlighted in the new Commonwealth Fraud Control Guidelines which outlined requirements to detect fraud and recommended data mining and matching as a fraud detection technique.<sup>8</sup>

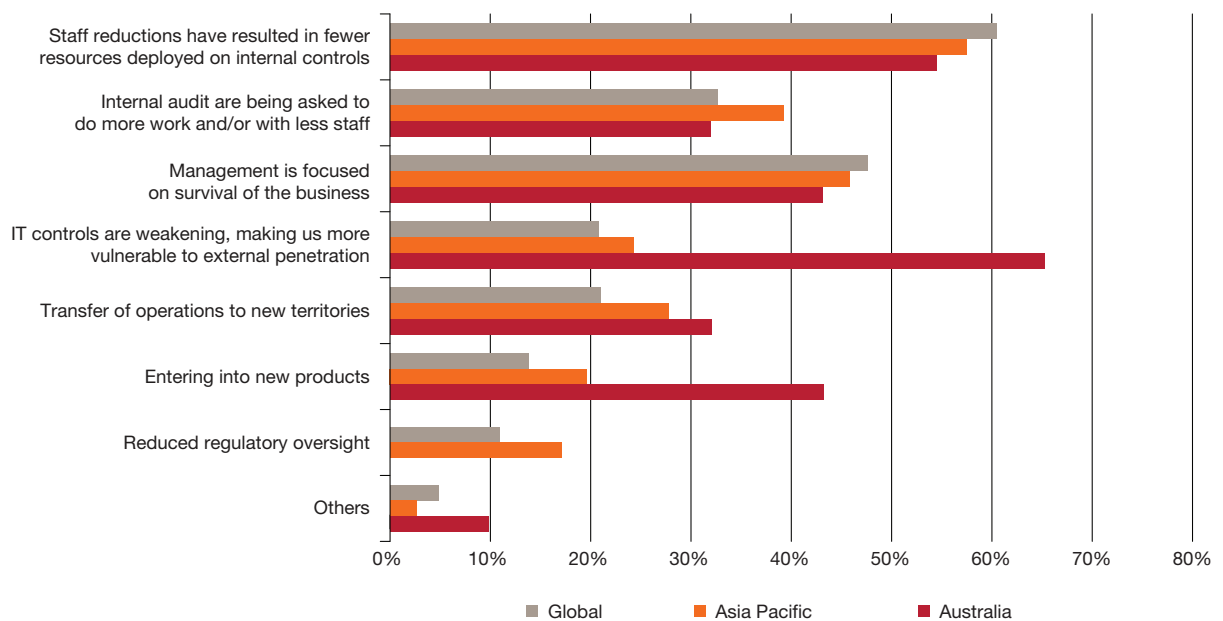
As shown in Figure 7, diminished IT controls and staff reductions in Australia across all industries are seen as presenting the greatest opportunities for perpetrators of economic crime.

## Pay, performance and fraud

Linking pay to performance is another possible driver of fraudulent activity. Organisations need to be aware of the correlation between compensation structures and heightened fraud risk.

According to the PwC *Global Economic Crime Survey*, public sector organisations with a performance-related pay structure for senior executives are almost twice as likely to have reported fraud (44%) than those that make no link between pay and performance (27%). There is a clear link between the incentive performance related pay structures created and the instances of reported fraud.

**Figure 7: Factors given by respondents from all industries as contributing to increased opportunities to commit fraud**



<sup>7</sup> NSW Auditor-General's Fraud Control Report, page 5

<sup>8</sup> Commonwealth Fraud Control Guidelines 2011, page 15

# Prevent, detect, respond

## Prevention – your first line of defence

The foundation of any good fraud risk framework is a set of solid prevention strategies. ANAO fraud surveys found a significant improvement from 2002 to 2009 in the mechanisms government departments used to prevent fraud. These are shown in the table below.

<i>Mechanism</i>	<i>2002 ANAO survey %</i>	<i>2009 ANAO survey %</i>
Governance structures and staff allocated responsibility	94	100
Fraud policy statement	80	90
Fraud risk assessment	69	88
Fraud control plan	70	86
Procedures and guidelines	71	96
Fraud awareness-raising activities	94	98
Training in ethics or code of conduct	n/a	90
Training in privacy principles	n/a	81
Training to employees involved in fraud control activities	n/a	66

In Appendix A we have summarised the chief executive's obligations, risk assessment and fraud control plan requirements from the new Commonwealth Fraud Control Guidelines.

Despite these improvements, there is still work to do instituting fraud control plans in response to fraud risks, and in training employees in fraud control activities.

We also note the new Commonwealth Fraud Control Guidelines make no reference to pre-employment contractor screening and vendor screening. An area of great concern to employers is the identity of the people they employ. Pre-employment screening may reveal details of an individual's criminal convictions, but are these checks rigorous enough? The level of screening varies considerably – i.e. reference checking versus police checks. The checks themselves can also be vulnerable to fraud. For example, when calling a mobile phone to conduct a reference check how do you know who you are really talking to or the capacity in which they know the potential employee? Employees are often entrusted with extensive authority and autonomy without their employers knowing enough about their backgrounds.

Further best practice screening would include verification of qualifications, professional associations, media searches and in some instances court proceedings.

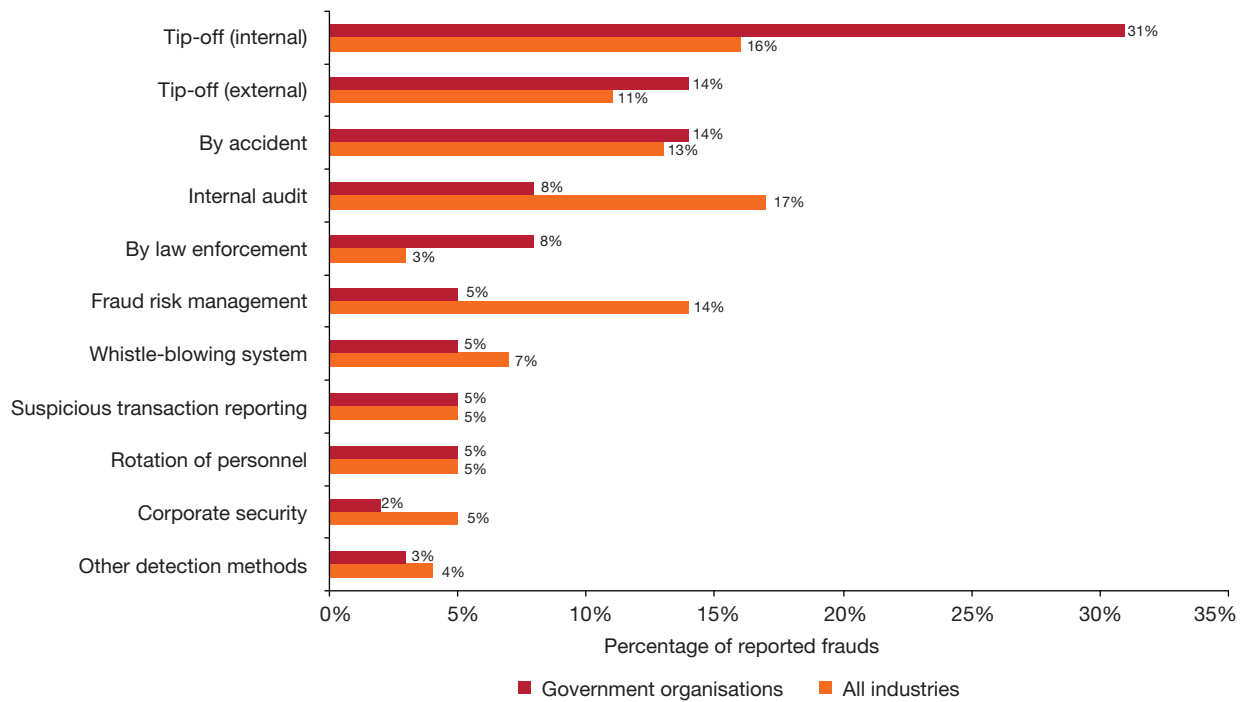
The issue of employee checks becomes particularly important when a project is outsourced to a third party. Government organisations must ensure that any party they contract with has appropriate policies and procedures in place to identify rogue employees, contractors or suppliers before they have the opportunity to compromise security. A number of public sector organisations have failed to grasp the concept that they retain the fraud risk even if they have outsourced the function. Consequently, they do not ask service providers about their risk assessment processes or employee due diligence arrangements.

Another prevention strategy is annual declarations by employees and potential suppliers. The declaration would state that the individual is not aware of any non-compliance with relevant policies and procedures. This may prompt staff to raise relevant issues, and provide an opportunity to refresh and improve staff awareness of policies and procedures.

## How is fraud being detected?

According to the *PwC Global Economic Crime Survey*, for the public sector, 31% of fraud is detected by internal tip-off and 14% by external tip-off, and 14% by accident.

**Figure 8: Detection methods**



**31%**

*of economic crime is detected from internal tip offs but only 5% through whistleblower systems. How can whistleblower systems be enhanced?*

## Internal audit

The AIC's survey found that 90%<sup>9</sup> of external fraud and 40%<sup>10</sup> of internal fraud is detected by internal controls, audit and investigation. This finding is in contrast to the PwC *Global Economic Crime Survey* that found that in government and state-owned enterprises, internal auditing was detecting only 8% of economic crime compared to all other industries at 17%. It is not clear why the difference but the effectiveness of internal audit will reduce with a reduction in staff dedicated to internal auditing, or internal audit resources being diverted from fraud detection to performance audit activities, or a combination of both.

Source of discovery	% Internal Fraud	% External Fraud
Internal controls / audit investigation	46	90
Staff member/ colleague discovered	8	0.5
Internal anonymous whistleblower	5	0.05
External whistleblower	29	9
External audit investigator	0.5	0.01
Notification by police	0.2	0.01
Offender self reported	1	0.00
Other	10	0.3

## Tip-offs and whistleblower hotlines

According to the PwC *Global Economic Crime Survey*, the strength of fraud detection at government organisations depends on informal processes, with 45% of fraudulent acts being detected through internal and external tip-offs. This compares with the all-industries average of 27%.

Even though 95% of Australian federal government agencies claim to have whistleblowing procedures,<sup>11</sup> we note that according to the PwC *Global Economic Crime Survey* a relatively large proportion of frauds were detected by accident (14%) and that only 5% were uncovered through formal whistleblowing procedures.

The AIC findings are not quite so bleak with 29%<sup>12</sup> of internal fraud and 9%<sup>13</sup> of external frauds being detected through an external whistleblower. That said, whistleblower channels can become more effective in terms of:

- staff awareness
- staff trust in the whistleblower process
- maintenance of the channels – for example, in one recent investigation, PwC was provided with a whistleblower email account, only to find it was inactive.

In addition, according to the ANAO survey, only 45% of agencies indicated that they had fraud 'tip-off lines' in place to facilitate reports from members of the public about potential fraud.<sup>14</sup> This was confirmed in New South Wales, where the Auditor-General's survey found that 68% of its agencies and universities had "less than effective" consumer and community fraud awareness programs.<sup>15</sup>

The new Commonwealth Fraud Control Guidelines have specified that employees, clients or members of the public must be provided with an appropriate channel for reporting fraud that, where possible, ensures confidentiality.<sup>16</sup>

<sup>9</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, Table 20

<sup>10</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, Table 11

<sup>11</sup> ANAO'S Fraud Control Report, page 89

<sup>12</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, Table 20

<sup>13</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, Table 11

<sup>14</sup> ANAO'S Fraud Control Report, page 90

<sup>15</sup> NSW Auditor-General Fraud Control Report page 6

<sup>16</sup> Commonwealth Fraud Control Guidelines (CFCG) 2011, paragraph 10.4

## Fraud risk management and assessments

According to the PwC *Global Economic Crime Survey*, although most (61%) of government and state-owned enterprises had performed a fraud risk assessment during the year, this detected only 5% of frauds.

A report prepared by the New South Wales Auditor-General in 2010 and submitted to State Parliament found that of the 57 agencies and universities, most thought they had an effective fraud control policy. However:

- 22 respondents (39%) rated their fraud risk assessment processes and employee awareness programs as “less than effective”
- 23 respondents (40%) rated their detection systems as “less than effective”<sup>17</sup>

While 91% of Commonwealth agencies reported to the AIC that they had completed a fraud risk assessment<sup>18</sup>, the ANAO survey reported that of the 160 Commonwealth agencies, only 54% stated their fraud prevention and detection strategies were effective. The other 46% of agencies had not evaluated the effectiveness of their strategies.<sup>19</sup>

While there is an argument that risk management and appropriate controls may mitigate the risk of fraud, the fact that the public sector reported higher overall fraud than other industries suggests governments could make improvements including those recently specified in the Commonwealth Fraud Control Guidelines such as:

- adopting more thorough fraud risk assessments to identify a range of risks
- updating and reviewing fraud assessments with any change in the business, such as the addition of a new structure or business unit,<sup>20</sup> deployment of a new program,<sup>21</sup> heightened risk or a change in incident levels
- addressing identified risks by corresponding fraud prevention plan strategies.

The practice of simply “reviewing” old fraud risk assessments and fraud control plans in order to save money is unlikely to be a robust prevention strategy.

### **Fraud risk assessment**

*In our experience and based on the recently released Commonwealth Fraud Control Guidelines, a comprehensive fraud risk assessment should:*

- *identify the potential inherent fraud risks*
- *assess the likelihood and significance of the identified risks occurring*
- *identify existing preventative and detection controls and map them to the relevant fraud risks*
- *evaluate whether relevant controls and processes are designed to address identified fraud risks effectively*
- *identify and evaluate residual fraud risks resulting from ineffective or non-existent controls*
- *assign individual responsibility to manage and respond to residual fraud risks*
- *update fraud risk assessments at least every two years and more frequently as new programs and initiatives are introduced.*



<sup>17</sup> NSW Auditor-General Fraud Control Report page 6

<sup>18</sup> Australian Institute of Criminology Fraud against the Commonwealth 2008-2009 Annual Report to Government 4 April 2011, page 16

<sup>19</sup> ANAO Fraud Control Report, page 16

<sup>20</sup> Commonwealth Fraud Control Guidelines 2011, paragraph 6.8

<sup>21</sup> Commonwealth Fraud Control Guidelines 2011, paragraph 6.9

## Data analytics

A powerful way to detect fraud is to use transaction monitoring and data analytics to identify unusual transactions that occur through error, control weakness or fraud.

Data analytics employs sophisticated software to interrogate transaction data for known fraud traits or breaches of controls. Any data can be analysed, but this method is most typically applied to accounts payable, payroll, corporate credit cards, superannuation payments, insurance claims and cash receipts.

It involves looking for unusual relationships between vendors and employees such as shared bank accounts or addresses, unusual payments such as before invoice date, out of hours, rounded amounts, frequent repeat amounts, consecutive invoice numbering, or no GST. More advanced techniques can monitor unusual transactions in real or near-real time.



### **Data analytics – Expense claims**

*Data analytics has been used to review unusual expense claims by employees, such as matching situations of claims for a travel allowance in addition to claiming travel cost; a claim through expenses and processing the invoice through accounts payable resulting in its employee receiving a credit for expense reimbursement and a credit from the vendor for the duplicate payment.*

### **Data analytics uncovers suspect rebates**

*Government rebate programs have used data analytics to identify unusual transactions, such as shared name, address and contact details and clustering of claims by date, location and type of claim. When transaction details are in the millions, data analytics is the only meaningful way to fully analyse the vast amount of information and identify suspicious transactions. Data analytics allows unusual payments to be identified and recovered or stopped.*

### **Data analytics – Break point clustering**

*Data analytics has been used to identify invoice payments and purchase orders that have been split to avoid delegations of authority limits. This involves data analysis of payment patterns to vendors and approved authorities.*

### **Data analytics – Allowance and overtime claims**

*Data analytics has been used to identify improper claims by employees for allowances and overtime. Allowances are analysed for the amount and number of claims within a period and compared to other employees. Overtime is analysed by reviewing hours claimed, matched to approval records and analysis of rates and frequency.*

## Response: sending the right message?

Many organisations claim to have a ‘zero-tolerance’ policy for dealing with internal fraudsters. In practice, this is not always the case. The *PwC Global Economic Crime Survey* revealed that the perpetrator faced dismissal in only 51% of reported frauds during the year. In addition, only 40% of cases resulted in civil or criminal charges.

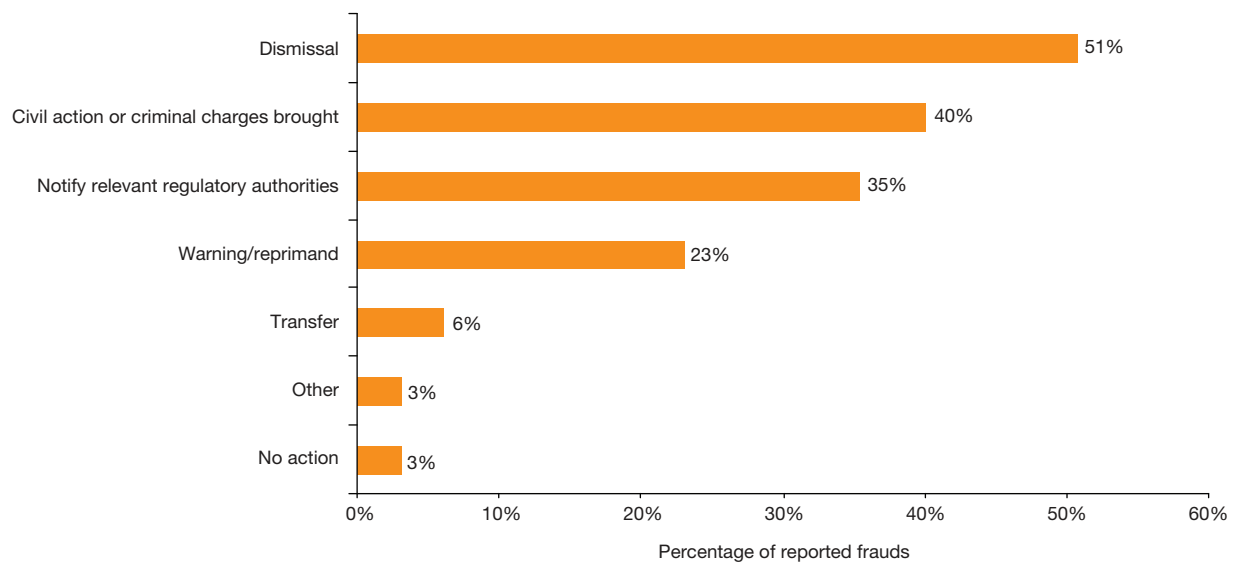
In our experience, organisations are often reluctant to bring charges against employees because of the time and costs of developing a case and the lack of reliable records upon which to base a prosecution. But this attitude may leave fraudsters free to commit crimes again.

## Are there other considerations when deciding how to deal with a fraudster?

If the suspected individual is a senior executive or in cases where a complex fraud has been committed, organisations may be reluctant to take action – particularly if it might compromise service delivery. Across all industries, 60% of internal fraudsters faced dismissal, but the public sector seems less willing to use dismissal as a way of addressing fraudulent behaviour. Unfortunately the lack of visible action might send a message to other staff that management tolerates this type of behaviour. It may also explain why official routes for reporting fraud are used less in government and state-owned enterprises than in other sectors.

There is also the risk that employees who have been disciplined by one department, but not dismissed, may go to work for another area of government and continue their fraudulent behaviour. To avoid this situation, government bodies might consider a central fraud-reporting process and include security vetting for employees.

**Figure 9: Actions taken against internal fraudsters by government and state-owned enterprises**



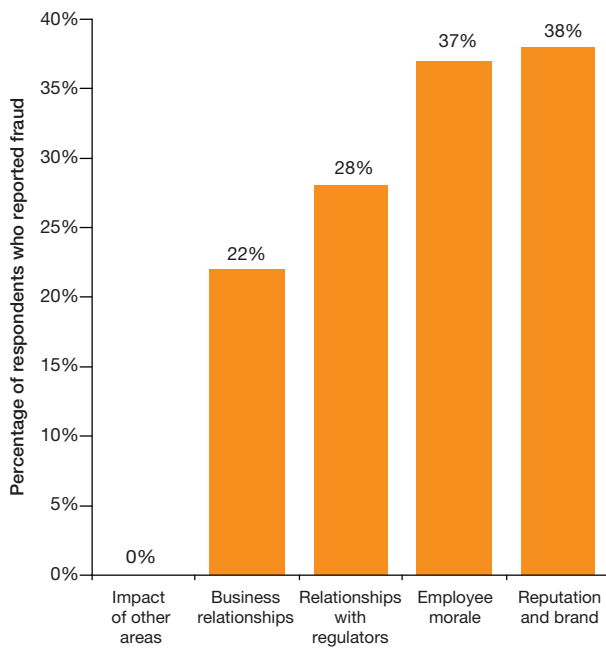
## Collateral damage

The fall-out from fraud goes beyond economic cost. Our survey also examined the collateral damage suffered by organisations and asked what impact economic crime had on their reputation and brand, employee morale, business relations and relations with regulators.

Most respondents did not see collateral damage as having a significant impact on their organisation, perhaps because it is difficult to quantify such costs. However, according to the PwC *Global Economic Crime Survey*, the most damaging impact of fraud is on reputation and brand (reported as “very significant” or “significant” by 38% of respondents) and employee morale (reported as “very significant” or “significant” by 37%).

While it is difficult to quantify the cost of such collateral damage, it can ruin careers by association and should be of real concern to organisations. Negative media coverage arising from fraud may deter employees, investors, suppliers, customers and potential recruits.

**Figure 10: Collateral damage as reported by government and state-owned enterprises**



## Setting the tone at the top

We strongly believe senior executives should take an active interest in fraud risks within their organisation. By demonstrating the highest ethical behaviour and engaging with the business in relation to fraud risks – and undertaking robust enforcement action against the perpetrators of fraud – they can establish the right ‘tone at the top’.

Conversely, senior executives who appear unconcerned about fraud may unwittingly foster environments where types of fraud are perceived to be permissible.

When senior executives do not convey an appropriate message and reinforce it through appropriate actions and behaviours, fraud can have a much more damaging impact on an organisation. The complex cultural challenges that arise in the fight against fraud can only be overcome if the workforce has been equipped with the right skills.

A crucial part of this process involves senior executives empowering and motivating employees to do the right thing, because it is the right thing to do.

Non-executive directors also have an essential role in setting the tone at the top and must ensure that they use an organisation’s governance structure to reinforce management’s messages of honesty and integrity. An effective audit committee should be aware of fraud risks and take actions to ensure the organisation is appropriately managing these risks.

*Often collateral damage can have a greater impact on the organisation than the economic crime itself*



# What's on the fraud horizon?

*When asked about the most likely fraud threats in the following 12 months, respondents from government and state-owned enterprises identified asset misappropriation, accounting fraud and bribery and corruption. These outcomes are hardly surprising, since they were the most commonly experienced frauds during the preceding 12 months.*

However, 21% of respondents also felt their organisation was “quite likely” or “very likely” to experience intellectual property infringement (including loss of data) in the next 12 months. The nature and extent of the personal data that government organisations hold makes them a key target for fraudsters.

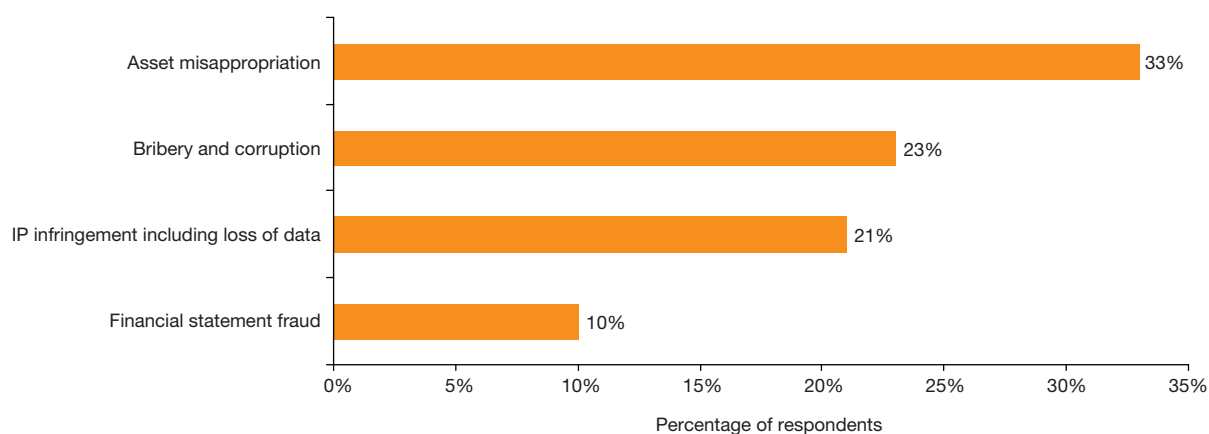
Similarly, the ANAO report identified the following ongoing and emerging fraud risks:

- unauthorised or inappropriate use of information technology
- unauthorised access to and release of information
- forgery or falsification of records
- identity fraud
- outsourcing of service delivery
- introduction of new policy initiatives and programs
- introduction of internet-based transactions and electronic information exchanges.

Based on our experience working in this sector, we further identify procurement fraud to be another fraud risk on top of those reported in the ANAO report, which ranges from the tender process to invoicing and payment. We are also increasingly working with clients in the corporate sector on their proof-of-leave balances and leave taken. Employee leave is not being recorded or categorised properly and this is distorting the internal financial records. This is emerging as a new fraud risk in that environment and we expect to see it emerge in the public sector in the next few years.

In response to these ongoing and emerging fraud risks, organisations must ensure they take the steps necessary to ensure they are well protected against the most common types of fraud and regularly review their fraud risk assessments.

**Figure 11: Perception of fraud in the next 12 months in government and state-owned enterprises**



# Conclusion

*Our statistics indicate that the public sector is trailing the private sector in the number of frauds detected by internal audit or risk management. Our experience in the private sector has shown that effective use of certain tools, such as transactional analytics and whistle-blowing programs, can be an important part of the fight against fraud. For example, investing in IT techniques such as data analytics, and conducting a comprehensive fraud risk assessment of your operations will be of benefit. Responsibility for preventing, detecting and responding to fraud lies with all employees in the organisation, within the context of their own particular role, but must be led from the top.*

We have identified six key action points for the government sector:

1. Ensure fraud risk assessments are comprehensive and not just a 'tick the box' exercise.
2. Regularly update risk assessments to reflect changes to the business, especially when new programs are introduced.
3. When risks are identified, implement a comprehensive fraud plan that includes nominating a person responsible for addressing the risk, implementing systems to monitor the risk, and considering alternative controls to mitigate the risk.
4. Using data analytics can greatly assist with fraud detection – government agencies should enhance their search routines to correlate suspicious information and enable intelligent analytics.
5. Staff who manage payments, procurement and contracting processes should receive fraud-specific training, as the organisation can be protected against many forms of fraud through their diligence.
6. CEOs and lead executives should become visible in their leadership of fraud control strategy to set the right tone from the top.

*Our experience in the private sector has shown that effective use of certain tools, such as transactional analytics and whistle-blowing programs, can be an important part of the fight against fraud*



# Methodology

The fifth PwC Global Economic Crime Survey was conducted between July and November 2009. A total of 3,037 respondents completed the online questionnaire; of these, 177 were from government and public sector organisations. The participants were asked to answer questions regarding (a) their organisation and (b) the country in which they are located.

**Table 1: Participating territories**

Argentina	1
Australia	14
Austria	1
Belgium	2
Brazil	1
Canada	3
Chile	2
Czech Republic	2
Ghana	5
Greece	6
Hong Kong and China	5
Hungary	2
India	1
Indonesia	1
Ireland	12
Italy	3
Kenya	4
Malaysia	1
Mexico	2
Netherlands	11
New Zealand	18
Norway	1
Poland	2
Russia	1
Singapore	1
Slovakia	1
South Africa	7
Spain	2
Sweden	5
Switzerland	13
Ukraine	1
United Kingdom	44
USA	1
Sierra Leone	1
<b>Total</b>	<b>177</b>

**Table 2: Size of participating government and state-owned enterprises**

	Percentage of organisations
Up to 200 employees	23%
201 to 1,000 employees	32%
More than 1,000 employees	44%
Don't know	1%

**Table 3: Function (main responsibility) of participants from government and state-owned enterprises**

	Percentage of organisations
Executive management or finance	42%
Audit	23%
Risk management	6%
Advisory or consultancy	6%
Operations and production	5%
Compliance	4%
Security	4%
Others	10%

**Table 4: Job title of the participants from government and state-owned enterprises**

	Percentage of organisations
Senior executives	40%
Chief Executive Officer/President/Managing Director	7%
Chief Financial Officer/Treasurer/Controller	26%
Chief Operating Officer	2%
Chief Information Officer/Technology Director	1%
Other senior executive	2%
Board member	2%
Non-senior executives	60%
Senior Vice President/Vice President/Director	4%
Head of business unit	8%
Head of department	15%
Manager	19%
Others	14%

## Terminology

Due to the diverse descriptions of types of economic crime in countries' legal statutes, the following categories were developed for the purpose of the survey. These descriptions were defined as such in the survey questionnaire.

### ***Economic crime or fraud***

Intentionally using deceit to deprive another of money, property or legal right.

### ***Asset misappropriation (including embezzlement or deception by employees)***

The theft of assets (including monetary assets, cash or supplies and equipment) for their own benefit by directors, others in fiduciary positions, or employees.

### ***Accounting fraud***

Altering financial statements or other documents, or presenting them in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings or raising of finance, fraudulent applications for credit and unauthorised transactions or rogue trading.

### ***Corruption and bribery (including racketeering and extortion)***

Unlawfully using an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to accepting such inducements.

### ***Money laundering***

Actions intended to legitimise the proceeds of crime by disguising their true origin.

### ***Intellectual property infringement (including trademarks, patents, counterfeit products and services)***

This includes illegally copying or distributing fake goods in breach of patent or copyright, and creating false currency notes and coins with the intention of passing them off as genuine.

### ***Illegal insider trading***

Buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about that security. Insider trading may also include 'tipping' such information, securities trading by the person tipped, and securities trading by those who misappropriate such information.

### ***Espionage***

The act or practice of spying or of using spies to obtain secret information.

### ***Financial performance***

Measuring the results of an organisation's policies and operations in monetary terms. Typically, returns will be measured in terms of service delivery.

### ***Fraud risk assessment***

These are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

- the fraud risks to which operations are exposed
- an assessment of the most threatening risks (i.e. evaluating risks for significance and likelihood of occurrence)
- identification and evaluation of the controls (if any) that are in place to mitigate the key risks
- assessment of the general anti-fraud programs and controls in an organisation
- actions to remedy any gaps in the controls.

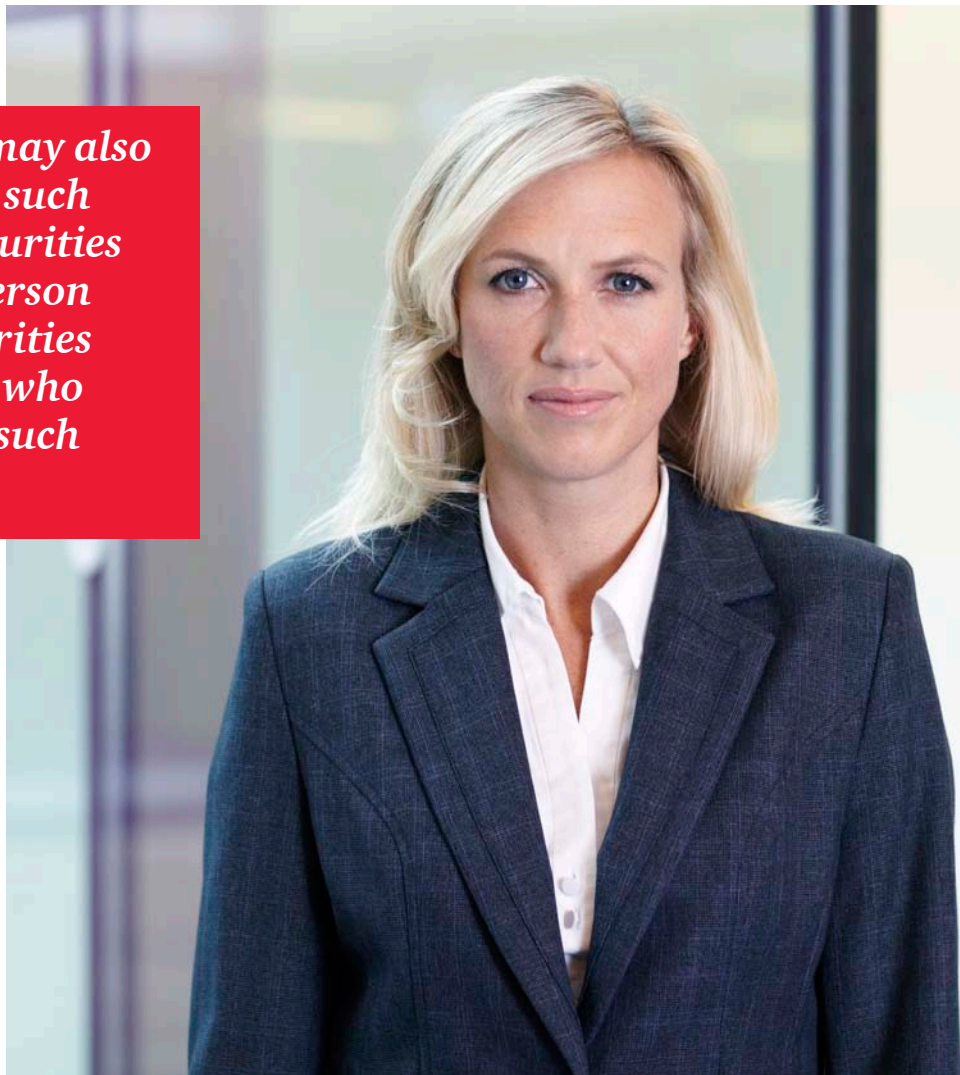
### ***Fraud triangle***

The interconnected conditions that act as harbingers to fraud: opportunity to commit fraud, incentive (or pressure) to commit fraud, and the ability of the perpetrator to rationalise the act.

### ***Senior executive***

The main decision-maker in the organisation (for example the CEO, Managing Director or Executive Director).

***Insider trading may also include ‘tipping’ such information, securities trading by the person tipped, and securities trading by those who misappropriate such information***





---

# *PwC Forensic Services: An Overview*

*PwC's Australian Forensic Services team offers a full spectrum of forensic solutions, ranging from fraud prevention and detection management to post-incident investigative services and remedial activities.*

Our team of forensic specialists includes:

- former regulators
- law enforcement agents
- forensic accountants
- computer forensic consultants
- research specialists

all of whom are highly experienced across a full range of industries.

The majority of our team are Certified Fraud Examiners and hold Certificate III in Investigative Services, Certificate IV in Government Investigation and Fraud Control and Commercial Agents and Private Inquiry (CAPI) licences.

We have access to over 1,400 staff and partners across PwC's global investigations and forensic services practice. All are experienced in our service offerings, across all industries. Therefore we are able to provide clients in any industry with timely, high quality, practical and commercial resolutions to any forensic issue.



# Appendix A

## Commonwealth Fraud Control Guidelines 2011

*Summary of Chief Executive's obligations, risk assessments and fraud control plan requirements*

### 5. Obligations of Chief Executives

- 5.2** Agency Chief Executives must manage the affairs of the agency in an efficient and ethical manner.
- 5.2** The fraud control plan may be a standalone or form part of the agency's risk management framework.
- 5.4** A Chief Executive must implement a fraud control plan for the agency, which addresses relevant risk factors and is updated on a regular basis.
- 5.7** Chief Executives must be satisfied that their agency complies with the mandatory requirements that are contained in the guidelines. eg risk assessments, fraud control plans, fraud detection, etc.
- Chief Executives must also:
- foster and maintain the highest standards of ethical behaviour in their agency
  - take all reasonable measures to prevent and detect fraud
- 5.8**
- ensure that program design and policy development incorporate consideration of fraud risks
  - report annually to their Minister or Presiding Officers on fraud risk and control measures
  - certify in their Annual Reports that they are satisfied with measures in place to control fraud.

### 6. Risk Assessment

- 6.1** Agencies must undertake a fraud risk assessment (internal and external risks) at least once every 2 years.
- 6.1** Agencies that undertake high fraud risk functions should assess risk more frequently.
- 6.2** Fraud risk should be considered as an aspect of the agency's broader risk assessment processes.
- 6.3** The likely occurrence of fraud and its impact on an agency must be carefully assessed.
- 6.3** Risk management should be integrated into an agency's strategic and business planning processes.
- 6.4** Risk assessment processes should acknowledge all factors likely to affect an agency's exposure to risk.
- 6.5** Management of fraud risks should be embedded in an agency's risk procedures. In some large agencies an additional fraud risk assessment specific to a particular policy or program area should be considered.
- 6.6** In developing their fraud risk assessment and control plan, agencies should adopt a methodology consistent with the relevant recognised standards.
- 6.7** Agencies should introduce a rolling program of updating risk assessments and mitigation measures. Agencies should develop dynamic risk assessment procedures within a general business risk approach.
- 6.8** Where an agency undergoes a change in structure, they must undertake another fraud risk assessment.
- 6.9** The risk of fraud must be considered when major new or changed policies are being developed.
- 6.9** The assessment of fraud risks should include measures to prevent fraud from occurring.
- 6.11** If the tasks are outsourced, the process must be overseen by a senior officer in that agency.
- 6.11** Agencies should ensure the outsourcing organisation meets the competencies set out in the Guidelines. Agencies should ensure that corporate knowledge is appropriately captured during the risk processes.
- 6.12** Agencies must review and refine their risk assessment strategies on an on-going basis.
- 6.12** The outcomes of fraud risk assessments should be provided to agencies' internal audit units, for consideration in the annual audit work program.

## 7. Fraud Control Plans

- 7.1** Fraud risk assessments must be followed by the development of a fraud control plan.
- 7.1** Effective mechanisms should be in place to oversee the process of developing and implementing the fraud control plan. This should emphasise prevention measures to minimise the opportunity for fraud.
- 7.2** Fraud control plans should be integrated into the agency's strategic, business or risk management plan.
- 7.3** Fraud control plans must address the agency's individual needs, including prevention, detection, reporting, and investigation measures.
- Fraud control plans should document the agency's approach to controlling fraud at all levels. Prevention, detection, reporting, and investigation measures should include:
- a summary of the identified fraud risks associated with the agency's function
  - the treatment of strategies or controls put in place to mitigate the identified risks of fraud
  - information about implementation
- 7.3**
- everyone to report fraud or suspected fraud
  - strategies to ensure the agency meets its training requirements
  - mechanisms for collecting, analysing and reporting the number and nature of incidents of fraud within or against the agency
  - protocols setting out how the agency will handle suspicions of fraud.
- 7.4** Controls and strategies outlined in the fraud control plans should be adequate with assessed fraud risks. Controls should be reviewed on a regular basis to make sure they remain useful.
- 7.5** Fraud control arrangements should reflect the fraud risk profile of an agency or particular program. Small public sector agencies should adopt "fit for purpose" mechanisms to address specific fraud risks.
- 7.6** Fraud control plans must include review mechanisms to regularly evaluate the fraud control strategies.
- 7.7** Agencies must provide a copy of their fraud control plans to the AGD or the AFP on request.
- 7.7** Fraud control plans should be user-friendly and available to all relevant employees.

---

***pwc.com.au/forensics***

---

## **Contacts**

### **PwC Forensics Services**

#### ***New South Wales***

##### **Cassandra Michie**

*Partner, Sydney*

Phone: +61 2 8266 2774  
cassandra.michie@au.pwc.com

#### ***New South Wales***

##### **Malcolm Shackell**

*Partner, Sydney*

Phone: +61 2 8266 2993  
malcolm.shackell@au.pwc.com

#### ***Victoria***

##### **Steve Ingram**

*Partner, Melbourne*

Phone: +61 3 8603 3676  
steve.ingram@au.pwc.com

#### ***Victoria***

##### **Michael Cerny**

*Partner, Melbourne*

Phone: +61 3 8603 6866  
michael.cerny@au.pwc.com

#### ***Australian Capital Territory***

##### **Tony Grieves**

*Principal, Canberra*

Phone: +61 2 6271 9402  
tony.grieves@au.pwc.com

#### ***Queensland***

##### **David Harley**

*Principal, Brisbane*

Phone: +61 7 3257 8307  
david.j.harley@au.pwc.com

#### ***South Australia***

##### **Kim Cheater**

*Partner, Adelaide*

Phone: +61 8 8218 7407  
kim.cheater@au.pwc.com

#### ***Western Australia***

##### **Cameron Jones**

*Partner, Perth*

Phone: +61 8 9238 3375  
cameron.jones@au.pwc.com

© 2011 PricewaterhouseCoopers. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers a partnership formed in Australia, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

This document is provided by PricewaterhouseCoopers as general guidance only and does not constitute the provision of accounting, legal advice, tax services, investment advice, or professional consulting of any kind. The information is provided "as is" with no assurance or guarantee of completeness, accuracy or timeliness of the information and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will PricewaterhouseCoopers or its professionals be liable in any way to you or to anyone else for any decision made or action taken in reliance on the information or for any direct, indirect, consequential, special or other damages related to you or your use of information, even if advised of the possibility of such damages. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all the pertinent facts relevant to your particular situation.