

Fraud in the public sector

a PwC Public Sector Research Centre publication



Contents

	Introduction	5
1	The extent of economic crime in the last 12 months	6
2	The profile of a fraudster	9
3	Prevent, detect, respond	13
4	What's on the fraud horizon?	17
	Conclusion	19
	Methodology and acknowledgements	20
	Contacts	22



Introduction

We are pleased to present the government and public sector extract from our Global Economic Crime Survey. The survey scrutinised fraud and associated integrity risks during a period of considerable economic turmoil and investigated the root causes and the way in which they affect organisations worldwide.

With economic turmoil, new threats have emerged. When economic survival is threatened (either for the organisation or for the individual), the line separating acceptable and unacceptable behaviour can, for some, become blurred. In addition, fraud and other types of economic crime have become a focus of criminal activity in recent years; criminal organisations that profit from fraud view the current economic conditions as an opportunity, not a threat. The public sector now seems set to undergo a period of significantly reduced spending and financial strain.

In this climate, it is essential that government/ state-owned enterprises evaluate the fraud risks that they face and take action to manage these risks effectively. Our survey revealed that the top reason for an increased risk of economic crime in the current environment is the fear of job loss. With severe public sector spending cuts expected in the coming months, this risk is set to increase further and organisations must ensure that they are ready to face this challenge. It is important that senior management take a proactive approach to fraud risk management and strive to create a culture of integrity and openness that empowers all employees to 'do the right thing'.

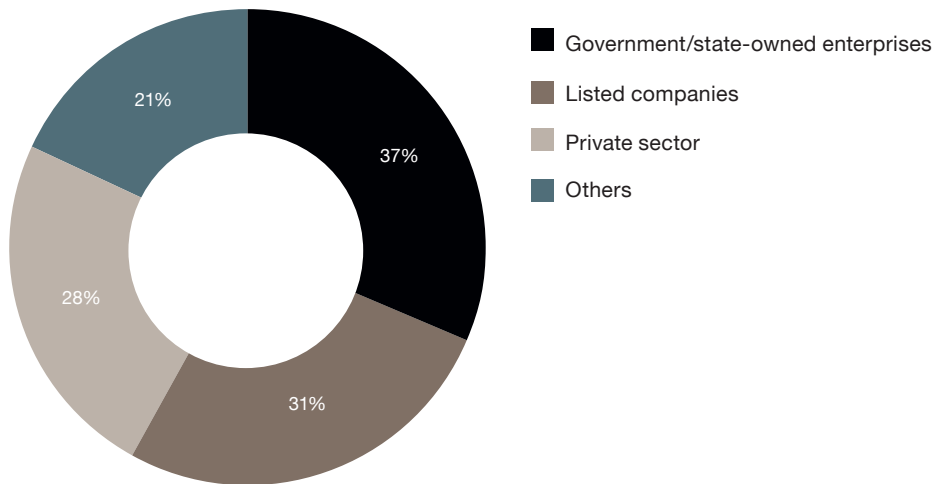
Survey participants

Over 170 senior representatives of government/ state-owned enterprises in 35 countries across the globe from Argentina to South Africa completed our web-based survey. Respondents were asked a number of 'core' questions on fraud and were also asked a number of other questions specifically on the fraud threats that emerge in an economic downturn. Further details of the survey demographics are presented in the 'Methodology and Acknowledgements' section of this report.

Note: In some cases percentages may total more or less than 100 percent as respondents were able to provide multiple answers.

The extent of economic crime in the last 12 months

Figure 1: % of organisations reporting fraud in the past 12 months



Globally, 37% of respondents from government/state-owned enterprises reported that their organisation had suffered economic crime in the last 12 months; higher than in any other type of organisation and the economic crisis has raised the perceived threat level of a fraud taking place, even higher.

This is despite the fact that only 41% of government/state-owned enterprises had suffered a decline in performance in the past 12 months compared to 62% of organisations in other sectors, however with increased public sector cuts on the horizon, the public sector believes that fraud could become an even bigger problem. This, in our experience, reflects the vulnerability that government/state-owned enterprises feel to external perpetrators of economic crime.

The number of government/state-owned enterprises reporting economic crime in the last 12 months rose to 52% and an even higher proportion (77%) believed that the economic crisis made fraud a greater risk to their organisation.

The impending reductions in spending that will cut a swathe across the public sector in the coming months and years will only serve to heighten the risks they face. There is no question that the public sector generally is entering a new and difficult era. Fears about job losses and achieving tough targets may drive people to take drastic steps. All organisations therefore need to be alive to the risks and ensure that they are well-prepared for the challenging future that lies ahead.

What kind of fraud is likely?

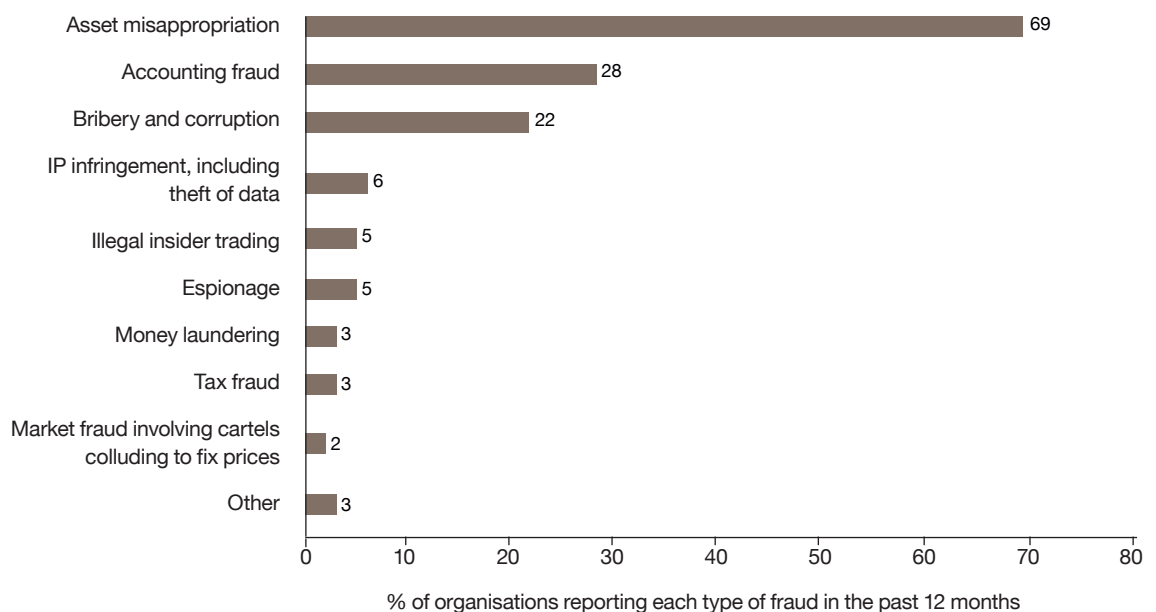
Economic crime takes on many different forms, some more common than others. The table below shows the types of economic crime suffered by those respondents who reported experiencing it in the last 12 months.

Over two-thirds of those reporting economic crime suffered asset misappropriation. This type of fraud is by far and away the most prevalent and covers a variety of misdemeanours. Whilst it is the hardest to prevent, it is arguably the easiest to detect.

Accounting fraud encompasses a variety of actions including accounting manipulations, fraudulent application for credit and unauthorised transactions.

Across the globe, 22% of respondents from government/state-owned enterprises experiencing economic crime reported cases of bribery and corruption in the last 12 months. In recent years there has been a global sea change in attitudes towards bribery and corruption, resulting in increased regulatory enforcement. This trend is likely to continue as more territories introduce or strengthen anti-corruption legislation and/or strengthen enforcement actions in response to global pressures, such as the UK Bribery Act which introduces a new crime of “failure to prevent” bribery. This means that organisations who are unable to demonstrate that they have implemented “adequate procedures” to prevent corrupt practices within their ranks or by third parties on their behalf, could be exposed to unlimited fines as well as other collateral consequences.

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



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 UNCAC and the OECD 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;
- Creating effective legal systems for seizing, freezing and confiscating the assets or proceeds of a crime; and
- Developing transparency in government operations and public procurement, and establishing enforceable codes of conduct for government officials.

It's not just money...

Although our survey focused on the extent and consequences of economic crime, fraudulent behaviour extends further. Our experience shows that unethical behaviour, such as manipulating data to meet targets or excessive staff entertaining, is on the rise. In certain circumstances, these behaviours may be seen as acceptable, or even condoned by management, but such attitudes can undermine anti-fraud policies and contribute to a culture of non-compliance within an organisation.

After analysis of patient data at a major hospital, allegations were made that management were manipulating waiting lists in order to meet performance targets. Patients were being removed from the waiting list without their knowledge and records were being 'fudged' so that it appeared that patients were being treated within the required timeline. The widespread practice of this type of fraudulent behaviour can undermine management's efforts to promote ethical values throughout an organisation.

The profile of a fraudster

2

Who is committing fraud?

Addressing the question of who is more likely to commit fraud and the circumstances under which individuals may be tempted to 'cross the line' can help all organisations to focus their anti-fraud policies in the right areas. For example, senior managers under most pressure to achieve demanding targets may resort to unethical means to hit their goals. Fear of redundancy may drive some to commit fraud or a lack of adequate controls could present the opportunist with the chance to enrich themselves or others relatively free of the fear of detection. All the contributory factors to fraud are likely to increase in the public sector as a result of a much tougher economic environment.

Within government/state-owned enterprises around the world, fraud seems to be more of an internal than external phenomenon. Organisations that suffered from economic crime reported that 57% of perpetrators were internal and 37% were external. However, it is interesting to note that in the UK this trend was reversed with 52% of respondents reporting that economic crime was perpetrated by external fraudsters. This reflects a perception within the UK public sector that fraud is normally committed by external parties. However, organisations must make sure that they are not underestimating either the cost or the collateral damage caused by internal fraudsters.

Figure 3: Who committed the most serious economic crime in the past 12 months?

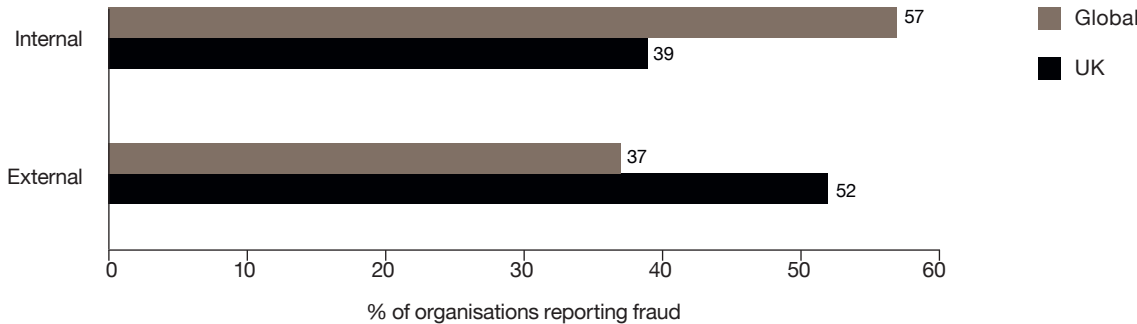
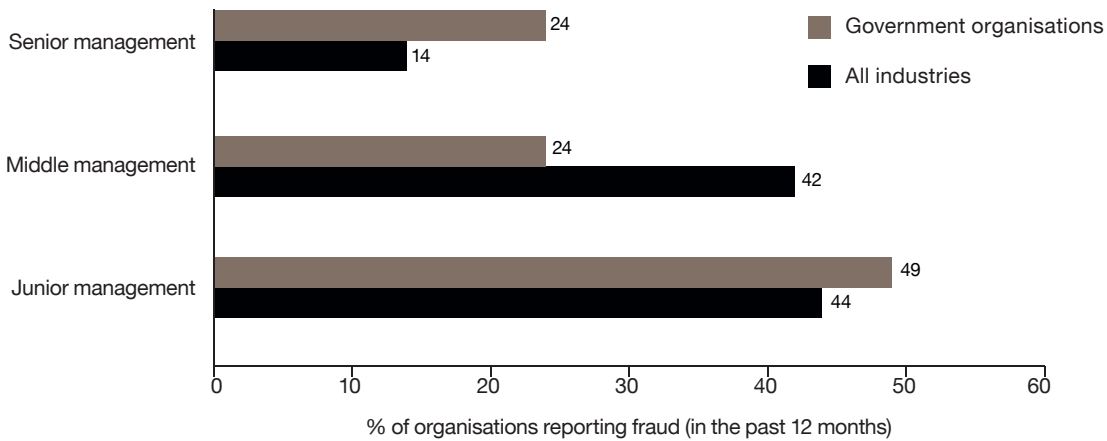


Figure 4: Profile of internal fraudsters

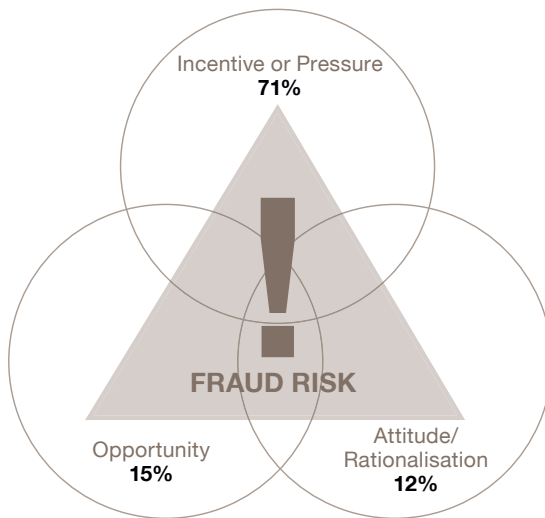


The number of economic crimes committed by middle management has risen sharply from 26% in 2007 to 42% in 2009 across all sectors. In contrast, within government/state-owned enterprises, the number of crimes committed by middle management has remained steady at 24%. In the public sector, junior management are most likely to commit fraud (49%) but a significant number of crimes were committed by senior management; more in the public sector (24%) than in other industries (14%).

Why are people committing fraud?

Fraud practitioners 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 needs to be an opportunity to commit fraud, and third, perpetrators are often able to rationalise or justify their actions.

The Fraud Triangle



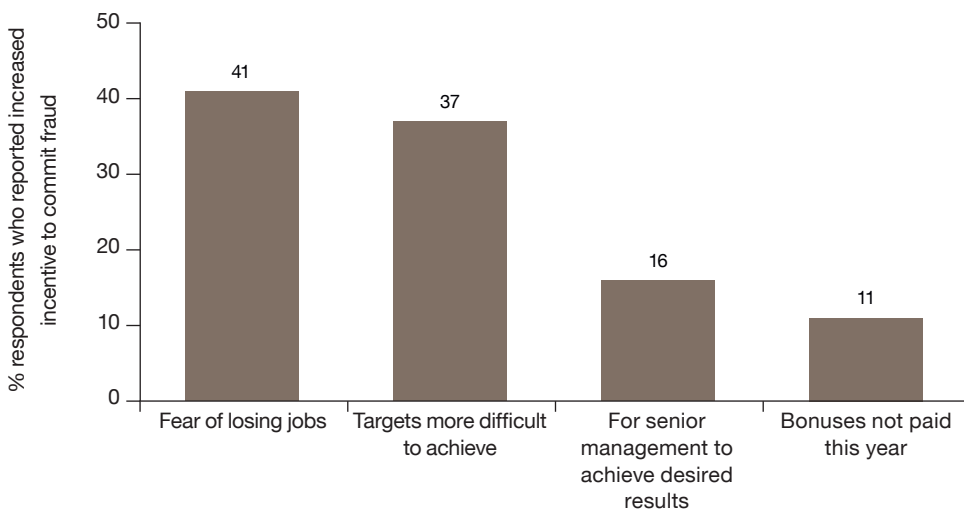
Probing deeper into the impact of these three factors reveals that among the respondents who believed that there is a greater risk of fraud in the current economic environment:

- 71% attributed greater risk of fraud to increased ‘incentives or pressures’;
- 15% reported that ‘more opportunities’ to commit fraud was the most likely reason for greater risk of fraud; and
- 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 very real fear of unemployment is a major pressure. The most commonly reported factor contributing to these increased incentives was that “people are afraid they might lose their jobs”. This pressure is set to increase with the expected cuts across the public sector in the next 12-18 months.

There was also concern that the current economic climate makes targets, both for individuals and organisations, more difficult to achieve. It is important therefore that organisations monitor performance closely and triangulate sources of information to identify when staff might feel under particular pressure.

Figure 5: Factors given by respondents from government/state-owned enterprises as contributing to increased incentives to commit fraud



A lack of control?

Of those respondents from government/state-owned enterprises perceiving greater opportunities to commit fraud in the current environment, 85% believed that staff reductions had resulted in fewer resources being deployed in internal controls. Financial difficulties force organisations to reduce costs and explore possible efficiencies. Staff reductions can result in reduced segregation of duties and less monitoring of suspicious transactions and activities. This, in turn, weakens the internal control environment and is often likely to result in more opportunities to commit fraud. It is important therefore that organisations consider how they employ their resources and ensure that sufficient investment is made in the prevention of economic crime and in tools, such as data analytics, that can help in the fight against fraud.

Pay, performance and fraud

Linking pay to performance is also likely to be a possible driver of fraudulent activity. Organisations therefore need to be aware of the correlation between compensation structures and a heightened fraud risk. According to the survey results, public sector organisations with a performance-related pay structure for senior executives are almost twice as likely to have reported fraud (44%) compared to those that make no link between pay and performance (27%).

Currently, 48% of government/state-owned enterprises reported that their compensation structure for senior executives contained no variable element linked to performance. As expected, this is significantly higher than the average of 16% across all industries but, as performance-related compensation structures become more common in the public sector, appropriate controls are important safeguards.

Do you know who your employees are?

One area of real concern to employers is the true identity of the people that they are employing. Organisations are increasingly finding that what were seen as 'trusted' employees have links to organised crime or terrorist groups. Pre-employment screening may reveal details of an individual's criminal convictions but are these checks really rigorous enough? Employees are often entrusted with a relatively large degree of authority and autonomy without the employer knowing enough about their background.

The issue of employee checks becomes particularly pertinent when a project is outsourced to a third party. Government organisations must ensure that any party they contract with has the appropriate policies and procedures in place to identify rogue employees before security can be compromised.

Prevent, detect, respond

3

How is fraud being detected?

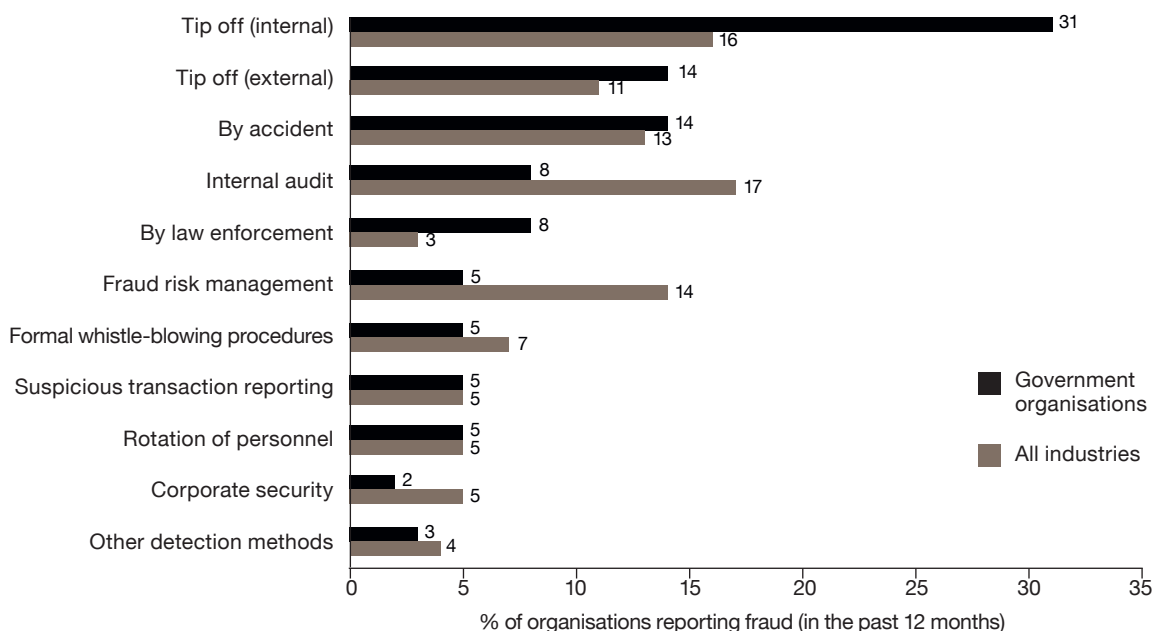
The survey suggests that the main factor contributing to the high levels of fraud in government/state-owned organisations is a lack of internal fraud prevention know-how and/or fraud prevention procedures.

The fact that a relatively large proportion of frauds were detected by accident (14%) reinforces this view with just 5% being uncovered through formal whistle-blowing procedures. 45% of organisations detected fraud through informal procedures via tip offs (both external and internal). This is higher than the global average of 27% and perhaps attributable to a lack of trust in formal procedures within the public sector arising from the poor track record of some organisations in dealing with whistleblowers.

Across all industries, internal audit proved to be relatively effective, detecting 17% of frauds. However, in government/state-owned enterprises, internal audit was less than half as effective, detecting only 8% of all frauds. Risk management procedures in the public sector picked up less than one-third of the frauds compared to their counterparts elsewhere.

Although the majority (61%) of government/state-owned enterprises had performed a fraud risk assessment during the year, only 5% of frauds were detected by fraud risk management procedures. While there is an argument that risk management may have resulted in mitigating controls, the fact that the sector reported higher overall fraud than other industries suggests that assessments are not being performed effectively. Robust fraud risk assessments are essential for identifying potential fraud threats and weaknesses in controls that create opportunities to commit fraud. Government/state-owned enterprises typically have challenging efficiency targets that are often set by government policy. Many of these organisations have been presented with increasingly tough cost-reduction targets in recent years, and these are expected to become even more onerous in the current economic climate. There is a danger that as fewer resources are employed in the fight against economic crime, more frauds will go undetected.

Figure 6: Detection methods



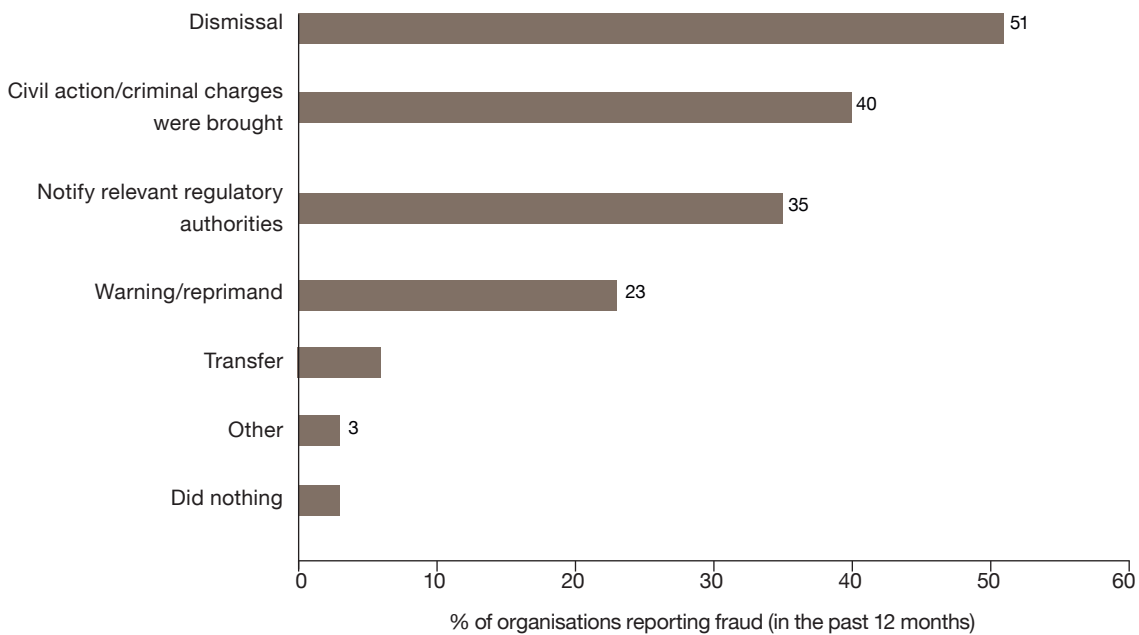
A comprehensive fraud risk assessment should:

- Identify the potential inherent fraud risks;
- Assess the likelihood and significance of occurrence of the identified risks;
- Evaluate which people and departments are most likely to commit fraud and identify methods they are likely to use;
- Identify and map existing preventative and detective controls to the relevant fraud risks;
- Evaluate whether relevant controls and processes are effectively designed to address identified fraud risks;
- Identify and evaluate residual fraud risks resulting from ineffective or non-existent controls; and
- Respond to residual fraud risks.

Response: sending the right message?

Many organisations claim to have a 'zero-tolerance' policy for dealing with internal fraudsters but does zero always really mean zero? Our survey shows that in only 51% of reported frauds during the year did the perpetrator face dismissal and in only 40% of cases were civil or criminal charges brought. In our experience, organisations are often reluctant to bring charges against employees because of the time and costs of developing a case. But this attitude may mean that fraudsters are free to commit their crimes again and again.

Figure 7: Actions taken against internal fraudsters by government/state-owned enterprises



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

If the suspected individual is a senior executive or a complex fraud has been committed, organisations may be reluctant to take action, particularly if it risks compromising service delivery. Across all industries, 60% of internal fraudsters faced dismissal but the public sector seems less willing to use this as a way to address fraudulent behaviour. Consequently, the lack of visible action may unwittingly send the message to other staff that this type of behaviour is tolerated by management. It may also explain why official routes for reporting fraud are used less by staff in government/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 on to work for another area of government without hindrance and continue their fraudulent behaviour elsewhere. To avoid this, government bodies must ensure that they are sufficiently joined up and share information appropriately.

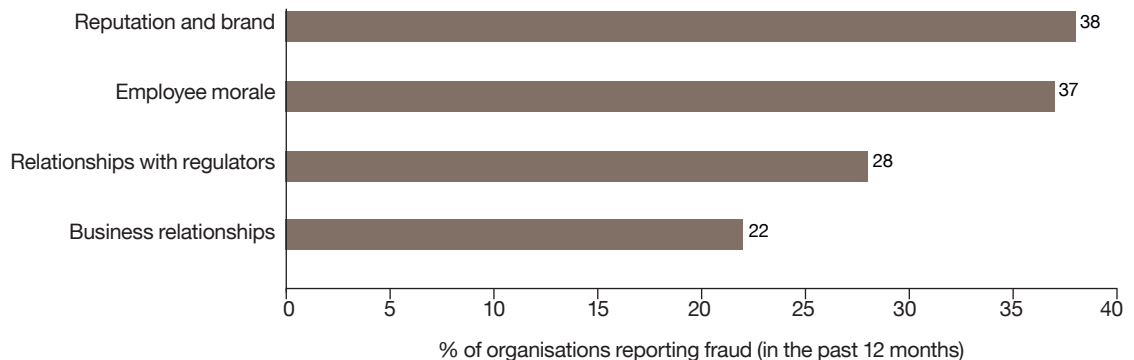
When an external fraudster is identified, the most common form of penalty is cessation of business relationships (in 17% of cases). Criminal/civil charges were brought to 40% of identified frauds.

Collateral damage

The fallout from fraud goes beyond economic cost. Our survey also investigated the collateral damage suffered by organisations and asked about the impact economic crime had on their reputation/brand, employee morale, business relations, and relations with regulators.

Most respondents do not see collateral damage as having a significant impact on their organisation, perhaps because it is very difficult to quantify such costs. However, most damaging, according to our survey, is the impact of fraud 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% of respondents). Whilst it is impossible to quantify the cost of such collateral damage, it should be of real concern to organisations. Negative media coverage arising from fraud can put off not just employees, but also investors, suppliers, customers and potential recruits.

Figure 8: Collateral damage as reported by government/state-owned enterprises



The tone from the top

Those at the very top of their organisations report less fraud than other employees, suggesting that they may not be sufficiently aware of the full extent of economic crimes in their organisation.

Fundamental to the fight against fraud is the attitude and ethical stance demonstrated by those at the top. If organisations want to get the 'tone at the top' right, senior executives need to be better informed about the fraud risks they are facing. Senior executives should ensure that they are proactive in their approach to fraud management and do not react only as a crisis hits. This failing is highlighted by the fact that while 60% of respondents to the survey were non-senior management, they reported 74% of the economic crime in the last 12 months. Is there complacency on the part of senior executives with regards to finance and operational matters or are they just disconnected from what happens 'on the ground'?

We strongly believe that senior executives should take an active interest in fraud risks within their organisation. By doing so, and by demonstrating high standards of ethical behaviour, together with robust disciplinary action where the perpetrators of fraud have been identified, the right 'tone from the top' can be established. Conversely, senior executives who appear unconcerned about fraud within their organisation may, through a lack of attention and focus, unwittingly foster environments where certain types of fraud are perceived to be permissible.

When the appropriate message from senior management is not conveyed and/or reinforced 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 management empowering and motivating employees 'to do the right thing, because it is the right thing to do'.

Non-executive directors, too, 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 that these risks are being appropriately managed.

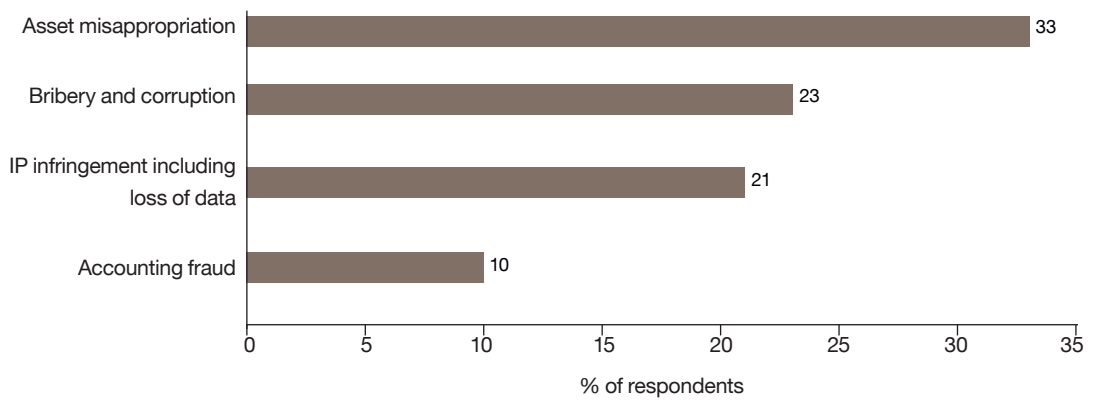
What's on the fraud horizon?

4

When asked about the most likely fraud threats in the next 12 months, respondents from government/state-owned enterprises identified asset misappropriation, accounting fraud and bribery and corruption. This is hardly surprising since these types of economic crimes were, after all, the most commonly experienced frauds over the last 12 months. In addition to these however, 21% of respondents felt that their organisation was 'quite likely' or 'very likely' to experience IP infringement (including loss of data) in the next 12 months.

The nature and extent of the data about people that government organisations hold makes them a key target for fraudsters. In response, organisations must ensure that they take the necessary steps to ensure that they are well-protected against the most common types of fraud and review their fraud risk assessments regularly.

Figure 9: Perception of fraud in the next 12 months in government/state-owned enterprises





Conclusion

In considering where to cut costs, organisations should reflect on the gaps within control procedures that will occur as the result of redundancies. Where there are fewer internal resources, such as the internal audit function or fraud risk management, to fight economic crime, more frauds will go undetected. Our statistics indicate that the public sector is trailing behind the private sector in terms of the number of frauds detected by internal audit or risk management. Our experience in the private sector has shown that the effective use of these tools can be an important part of the fight against fraud.

Investing in IT techniques, such as data analytics, at the beginning of a fraud risk assessment will be of benefit if your department is resourced constrained.

The incidence of fraud, be it external or internal, varies from country to country. Regardless of which type of fraud occurs, it is the individual's ability to rationalise their actions in the face of the situation they find themselves in that has increased the amount of fraud taking place. Therefore we suggest that an effective fraud risk assessment is carried out which will identify potential fraud threats and weaknesses. Our survey also revealed that redundancies result in reduced segregation of duties; indeed 15% of respondents reported that "more opportunities" to commit fraud were the most likely reason for greater risk of fraud.

Regardless of the fact that more internal fraud is being carried out, the risk assessment should cover both internal and external threats and weaknesses so all areas are covered.

We have also seen that zero tolerance does not always mean zero tolerance, with organisations often reluctant to bring charges against employees because of the time and costs associated with developing a case. If organisations are not prepared to bring criminal charges against individuals it will allow them to continue with their activities, whilst sending out a negative message to others. The tone from the top should make clear that these activities will not be tolerated once discovered and appropriate action will be taken.

We also suggest that government departments should be more joined up so when people do transfer departments, appropriate information can be shared about them.

Methodology and acknowledgements

Methodology

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

Table 1: Participating territories

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

Table 2: Size of participating government/state-owned enterprises

	% 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/state-owned enterprises

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

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

	% 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 individual types of economic crime in countries' legal statutes, the following categories were developed for the purposes of the survey. These descriptions were defined as such in the survey questionnaire.

Economic crime or fraud

The intentional use of deceit to deprive another of money, property or legal right.

Asset misappropriation (including embezzlement/deception by employees)

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

Accounting fraud

Financial statements and/or other documents are altered or presented 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/raising of finance, fraudulent applications for credit and unauthorised transactions/rogue trading.

Corruption and bribery (including racketeering and extortion)

The unlawful use of 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 the acceptance of such inducements.

Money laundering

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

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

Illegal insider trading

Illegal insider trading refers generally to 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 the 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

Espionage is the act or practice of spying or of using spies to obtain secret information.

Financial performance

This can be defined as 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

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

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

Fraud triangle

Fraud triangle describes 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 senior executive (for example the CEO, Managing Director or Executive Director) is the main decision-maker in the organisation.

Contacts

PricewaterhouseCoopers

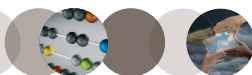


Billy O'Riordan
Partner
+353 1 792 8592
billy.oriordan@ie.pwc.com



Bob Semple
Partner
+353 1 792 6434
bob.semple@ie.pwc.com

Join the debate. www.psrc-pwc.com



The Public Sector Research Centre is PricewaterhouseCoopers' online community for insight and research into the most pressing issues and challenges facing government and public sector organisations, today and in the future.

The PSRC enables the collaborative exchange of ideas between policy makers, opinion formers, market experts, academics and practitioners internationally.

To register for this free resource please visit www.psrc-pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its Partners, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2010 PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the Irish firm, PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin1 which is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business. As the context requires, "PricewaterhouseCoopers" may also refer to one or more member firms of the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate legal entity. PricewaterhouseCoopers does not act as agent of PwCIL or any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way. Designed by PwC Design Studio 02722.

