

Cutting costs and cutting fraud

Economic crime in the public sector

*The results of our UK
survey of government
organisations.*

April 2011



Introduction

In July 2010 PwC published a report which examined the causes and extent of economic crime across the public sector. The report was based on responses to our fifth Global Economic Crime Survey, carried out in November 2009.

Since then the economic landscape of the public sector has changed considerably. The cuts which were widely predicted have become a reality, with government departments, local authorities and other public bodies having to make substantial cost savings, starting now.

We surveyed senior representatives from the public sector to find out how their experiences of economic crime had changed in the last 12 months and what effect they were expecting the Spending Review 2010 to have on their anti-fraud policies and procedures.

The results make startling reading. Since 2009, the number of organisations that have experienced some type of fraud has gone up to 60%. A recent report published by the National Fraud Authority estimated that the loss suffered by the public sector due to fraud was in the region of £21bn a year.¹

We have seen a big rise in accounting fraud; a crime which is often perceived to affect the private sector but, in our experience, is becoming increasingly pervasive in public sector organisations.

We expect that the effects of the Spending Review will result in an increased risk of fraud; a view shared by the majority of respondents to our survey. Despite this increased risk, nearly half of organisations said that there would be no change in their fraud prevention and detection methods. This is a dangerous game to play and experience tells us fraud could flourish in this type of environment.

Survey participants

Over 110 senior representatives from the public sector in the United Kingdom completed our web-based survey. Further details of the survey demographics are presented in the 'Methodology and Acknowledgements' section of this report.

¹ Annual Fraud Indicator 2011 published by the National Fraud Authority

The extent of the problem...

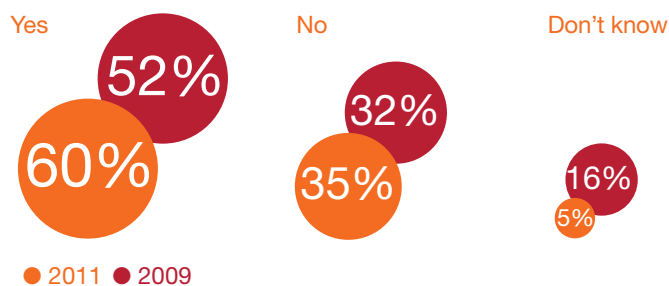
In November 2009, 52% of public sector organisations in the UK reported having experienced economic crime in the previous 12 months; far higher than the amount of fraud recorded globally for government/state-owned enterprises.

In the past 12 months, the number of organisations experiencing fraud has risen to 60%.

Historically, the most common type of fraud suffered has been asset misappropriation. Arguably this is the type of fraud that is both the easiest to detect and to prevent. However, for the first time, this has changed and the most common type of fraud – reported by over two-thirds of organisations that had experienced

fraud – is accounting fraud. This category of fraud encompasses a variety of actions including accounting manipulations, fraudulent application for credit and unauthorised transactions. In particular, we have seen a big rise in incidences of ‘accounting manipulations’ of which there were no reported incidences in 2009. This is often seen to be a victimless crime but, ultimately, it is the UK tax payer who pays the price.

Figure 1: Has your organisation experienced fraud in the past 12 months?



In the past 12 months, the number of organisations experiencing fraud has risen to 60%.

Figure 2: What type of fraud has your organisation experienced in the last 12 months?



What can you do to help spot accounting fraud?

One technique that can be used is the application of Continuous Transaction Monitoring (CTM). This technology leverages the huge volume of transactional data created by organisations – data that is rarely used to its full potential proactively to identify cost savings, improve business processes and detect fraud. Data analytics is not about using new information, but about using the information that you already have in a better way. When embedded in an organisation, CTM can act as

an early warning system for internal audit and Finance Directors by identifying predictive indicators of complex fraud schemes.

CTM technology applies data analytics, in near-real time, to transactions in a financial system to detect anomalies and identify areas of process inefficiencies. It can then help track appropriate remediation actions as part of an ongoing process. Automated analysis of these exceptions can provide you with quantitative information on which to make better, quicker business decisions. This results in cost savings ranging from reducing incidences of fraud and error through to improving business processes and controls.

In particular, we have seen a big rise in incidences of ‘accounting manipulations’ of which there were no reported incidences in 2009.

Case study

A local authority’s internal audit team applied CTM technology to provide visibility of process and control inefficiencies and to identify areas of fraud risk within the procurement function. CTM identified a broad range of anomalies and exceptions that had previously been unknown including duplicate invoice payments, false suppliers and unauthorised transactions. The internal audit team were able to demonstrate a quantifiable benefit to using CTM, saving the local authority a substantial amount of money.

Nearly a fifth of respondents reported having experienced bribery and corruption in the past 12 months. With the introduction of the Bribery Act, this type of fraudulent behaviour is expected to come under greater scrutiny. Later in this report we set out some of the main principles of the Act.

Of those who had reported experiencing 'other' types of fraud, over half had experienced benefit fraud. This area is increasingly becoming a focus of resources with the Department of Work and Pensions recently announcing a series of measures to combat fraud and error in the benefits system that could save £2bn a year. This is another area where data analytics could also help to achieve significant results for less expenditure by identifying duplicate payments and unusual patterns.

With the cost of fraud into the billions already, action needs to be taken now to address all types of fraud. With the restraints on both time and resources, the public sector needs to make sure that it is making the right decisions; it can't afford not to.

Direct payments and fraud

Local authorities are obliged to offer people who receive social services the option of direct payments in lieu of services. How these direct payments are spent, and who they are spent by, are areas of real concern. A number of organisations reported experiencing 'financial abuse of vulnerable adults' in the last 12 months. As the conditions attached to direct payments become more flexible, local authorities need to make sure that the processes are in place to identify any fraudulent use of funds and take action when required.

With the cost of fraud into the billions already, action needs to be taken now to address all types of fraud

organisation. Employment screening involves verifying the academic and professional history of candidates as declared during the application process, as well as seeking to identify any potentially adverse information which may be of interest to the prospective employer, for example an undisclosed criminal record. It shouldn't just apply to new employees though. In central government, where transfers between departments are relatively common, it can be easy for fraudsters to slip between the gaps and

simply move on before their crimes come to light. Organisations need to ensure that their HR and disciplinary procedures are up to date and sufficiently comprehensive to act as a deterrent.

Organisations are seeing the number of crimes committed by both internal and external fraudsters as either the same or greater than in 2009 with only 11% of respondents seeing the number of frauds as having reduced in the last 12 months.

Who is committing fraud?

In 2009, the majority of economic crimes were committed by external fraudsters, however in 2011 it appears that the majority of frauds were committed by employees; a statistic borne out by the increase in 'internal' crimes such as accounting fraud. Fraud is also pervasive throughout organisations from senior management to client facing 'on the ground' staff. Historically, the prevention of internal fraud has not been considered a priority for government but, as our survey results show, the risk from an organisation's own staff cannot be ignored.

Fraud can be extremely damaging both in financial terms and for an organisation's reputation. It is vitally important therefore that organisations know who they are employing and who is carrying out services on their behalf. The screening of potential employees can be a valuable risk management tool and is a highly cost effective way of minimising and guarding against potential security, financial and reputational risks by identifying undesirable or dishonest candidates before they join an

Figure 3: Who committed the most serious fraud of the past year?

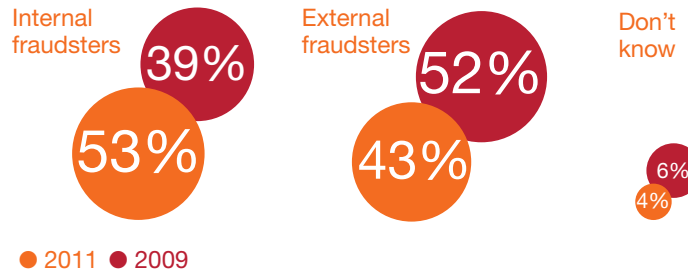
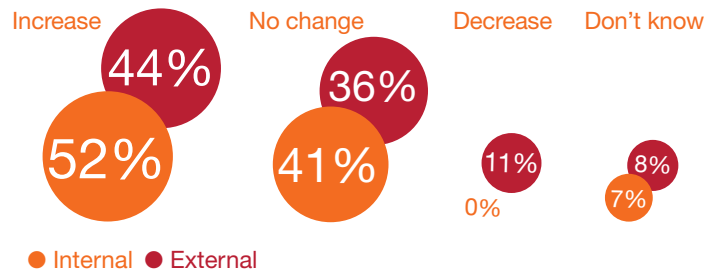


Figure 4: Has the amount of fraud committed by internal and external fraudsters changed in the past year?



The effects of the Spending Review 2010

The public sector has lived in the shadow of the Spending Review for many months and now organisations are beginning to implement the ensuing cuts to both the frontline delivery of services and the backroom functions. As the impact of the cuts begins to be felt, the pressure on individuals to act unethically is only going to increase, bringing with it a heightened risk of fraud.

In the current environment, 75% of respondents thought that the Spending Review would cause an increase in the risk of economic crime. Perhaps not surprisingly, nobody thought that one of the effects would be a decrease in the risk of economic crime.

In 2009, we asked what was the key factor driving the risk of a fraud being committed and 76% of respondents felt that there were ‘increased pressures and incentives to commit fraud in the difficult economic conditions’. Now that more details are known of what’s in store for the public sector, the number of people who felt that pressures and incentives would be the main driver of an increased risk of economic crime has fallen to 49%. Instead, the number of people who believe that there will be ‘more opportunities for frauds as costs are cut and gaps in control systems appear’ has risen from 15% to 36%. Similarly, the number of respondents who felt that people would be able to rationalise a fraudulent act has risen from 6% to 13%.

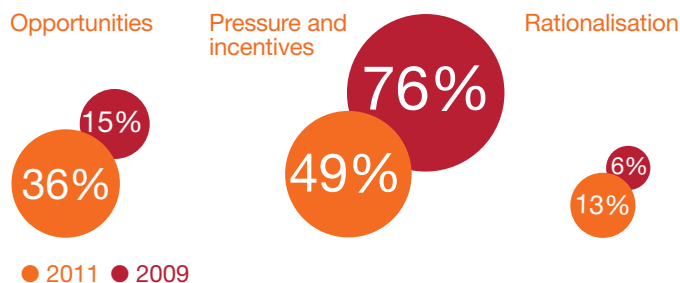
These three elements – opportunities, incentives and rationalisation – make up the so-called ‘fraud triangle’, created by Dr Donald Cressey, which represents the three factors which are generally present when a fraud occurs.

As the impact of the cuts begins to be felt, the pressure on individuals to act unethically is only going to increase bringing with it a heightened risk of fraud.

Figure 5: What impact do you think the Spending Review will have on the risk of fraud?



Figure 6: What is the key factor increasing the risk of fraud in the current environment?



It is clear that while there will always be the incentive for some people to commit fraud – and no more so than in times of redundancies and pay freezes – there is also a great deal of concern that fewer resources and cost-cutting may result in any gaps in a control framework being breached. In addition, the ability for some staff to rationalise a fraudulent act can often increase when they are threatened with redundancy; the ‘what have I got to lose?’ approach.

Despite the fact that the increased risk of fraud in the current environment was acknowledged by 75% of respondents (Figure 5), our survey found that 47% did not expect there to be any change in their organisation’s fraud prevention and detection methods as a result of the Spending Review. Fraud risk management

should be a fluid process, changing as necessary to adapt to the needs of the business. Organisations should ensure that they are continually re-evaluating their risk assessments and control processes so that they are focussing on the right areas; this is particularly important when resources are constrained.

Fraud risk management should be a fluid process, changing as necessary to adapt to the needs of the business.

Prevention & detection

As in previous years, informal tip offs continue to be the main means of detecting frauds in the public sector, perhaps attributable to the lack of trust in formal procedures and the poor track record of some organisations in dealing with whistleblowers. As a method of fraud detection however, it relies upon a series of coincidences – that somebody finds out about the fraud, that the person is compelled to do something about it, that they tell the right person – which are unlikely to come together in any systematic way.

One area of particular concern is the detection of procurement frauds. Recently publicised procurement frauds range in value from £500k to £3.6m, conducted over two-three year periods. Procurement frauds still occur because their prevention is often reliant on the vigilance of employees, and traditional detective measures can easily miss fraud that is hidden within millions of transactions and tens of thousands of suppliers.

Traditional detection techniques rely on ‘red flags’, such as transactions at weekends or late at night, which are well known to fraudsters and consequently can be easily avoided. They also often produce a large number of false positives resulting in a costly and time-consuming investigation. More advanced techniques rely on clustering data by a range of unusual supplier behaviours to identify subtle traces of a fraud, producing more accurate results which can be investigated more thoroughly.

Whistleblowing

It is encouraging to note that 26% of frauds were also reported through the formal whistleblowing process. Many organisations have made a concerted effort to encourage staff to make use of these resources and are beginning to see the results. There is no ‘one size fits all’ approach to the design and implementation of whistleblowing but it should form an important part of a wider strategy to promote openness and

transparency. An effective whistleblowing policy can also allow an organisation to become aware of a problem before it hits the headlines. All organisations should be concerned that employees have access to the channels to report any concerns that they may have and that there are procedures in place to investigate and manage the allegations appropriately.

Fraud Risk Assessments

In 2011, fraud risk management processes detected just 18% of frauds and in our survey we explored further the use of Fraud Risk Assessments (FRA); one of the key weapons in your anti-fraud toolkit. Robust fraud risk assessments are essential for identifying potential fraud threats and weaknesses in controls that create opportunities to commit fraud. 41% of respondents said that their organisation had never carried out a FRA which is worrying, given that The Institute of Internal Auditors calls this tool ‘a critical component’² of a risk management programme.

Top five methods of detecting fraud:

1. Internal tip off (40%)
 2. External tip off (28%)
 3. Whistleblowing (26%)
 4. Internal audit (26%)
 5. Risk management (18%)
-

² The Institute of Internal Auditors guidance, Internal Auditing and Fraud, December 2009

41% of respondents said that their organisation had never carried out a FRA which is worrying, given that The Institute of Internal Auditors calls this tool ‘a critical component’ of a risk management programme.

For those organisations that have carried out a FRA, we have concerns about the frequency with which they are being reviewed by the Audit Committee and senior management, including the Chief Executive and Board, with 21% of respondents admitting that the latter two had never reviewed their organisation’s FRA. Where it was reviewed, it was normally reviewed annually which, while better than nothing, may mean that an organisation’s risk assessment – and the understanding of that risk assessment – is out of date. In particular, 15% of respondents said that their FRA had never been reviewed by the Audit Committee; it is difficult to see how an Audit Committee can fulfil its function fully if its members do not have access to information about the risks facing their organisation and the processes that are in place to mitigate those risks.

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.*
- *Respond to residual fraud risks.*

Bribery Act

The Bribery Act 2010 represents a significant strengthening of anti-corruption legislation in the UK. While the real impact of the changes that it brings remains to be seen, no organisation can afford to ignore its implications.

73% of respondents to our survey considered the Bribery Act either ‘very’ or ‘quite relevant’ to their business. Surprisingly, given the coverage of the act to individuals, 12% of organisations felt that it was ‘not relevant’. There are some exemptions in the Act but any organisation that has any sort of commercial operations³ could fall foul of it. Public sector bodies must ensure that they are prepared as the repercussions of any breach of the Act could be very damaging. The Act promises unlimited fines both for individuals and corporations and lengthy jail terms for individuals. That is, obviously, in addition the damage done to an organisation’s reputation and credibility.

The Act itself is not complicated. In just 13 pages⁴ it outlines four corporate offences, three of which also apply to individuals, as shown in the table below.

These offences – whether for commercial organisations or for individuals – apply regardless of where in the world the bribes are offered or received, and can apply whether the bribery is direct or indirect, such as via a connected party such as an agent or joint venture partner.

It was reassuring to note that 73% of organisations had considered the implications of the Bribery Act on their activities but for the 15% who had not, the time to act is now.

Organisations need to conduct a thorough risk assessment, evaluate the existing procedures and address any control gaps before it is too late.

	Offence 1	Offence 2	Offence 3	Offence 4
	Paying or offering a bribe	Receiving or requesting a bribe	Bribing a foreign public official	Failing to prevent bribery on one’s behalf
Commercial organisations	✓	✓	✓	✓
Individual	✓	✓	✓	

The Act promises unlimited fines both for individuals and corporations and lengthy jail terms for individuals.

³ Defined as a body which carries on business, or part of a business, in any part of the United Kingdom (Bribery Act 2010, section 7.5)

⁴ <http://www.legislation.gov.uk/ukpga/2010/23/contents>

Conclusion

The public sector is undergoing a period of transformation and with any change programme comes increased risks. Our survey shows that the incidence of fraud in the public sector has risen since 2009 and that 60% of public sector organisations have experienced some form of fraud in the past 12 months. Unless action is taken now, this number will continue to rise.

We have also seen that the main threat to an organisation now comes from its own employees, with 52% of respondents seeing a rise in the number of crimes committed by internal fraudsters since 2009. Historically, the public sector has focussed on preventing and detecting crimes committed by external parties but organisations can't afford to ignore the threat posed by internal fraudsters.

As the effects of the Spending Review are felt across the public sector, our survey shows that respondents are expecting the risk of fraud to increase. There is an expectation that fraudsters will find more opportunities to commit fraud as control weaknesses are identified and exploited. There are also indications that the

economic climate is moving against the individual with rising fuel prices and the threat of increasing interest rates as well as the spectre of redundancies and pay freezes. In this environment, the very real threat to the livelihoods of thousands of individuals will increase the pressure on them to act dishonestly.

Organisations hold a large amount of data, particularly in relation to transactions, but many do not make full use of it. Techniques such as data analytics are of increasing interest as ways to identify excess costs and detect fraud, using information that an organisation already has. It can also be used in the fight against the growing risk of fraudulent accounting and manipulation.

Organisations must ensure that their limited resources are targeted appropriately to help mitigate the increased risk of fraud. For this, a comprehensive and regularly updated Fraud Risk Assessment is vital, identifying which types of fraud are most likely and what actions can be taken to help prevent these from occurring. We are also concerned that the incidence of fraud in the public sector is likely to become more invisible than ever as internal audit and fraud services are cut back, creating an environment where fraud is accepted as inevitable.

There is an expectation that fraudsters will find more opportunities to commit fraud as control weaknesses are identified and exploited.

Methodology and acknowledgements

Methodology

Our survey was conducted between January and February 2011. A total of 114 respondents from across the UK completed the online questionnaire. The participants were asked to respond to the questions regarding their organisation and where they were located.

Table 1: Location of survey respondents

England	98
Northern Ireland	8
Scotland	3
Wales	3
Other	0
Prefer not to say	1
N/A	1
Total	114

Table 2: Job title of participants (%)

Chief Executive Officer/President/Managing Director	4%
Chief Operating Officer	2%
Chief Financial Officer/Treasurer/Comptroller	14%
Senior Vice President/Vice President/Director	1%
Head of Department	4%
Head of Internal Audit	38%
Manager	12%
Other (please specify)	22%
Prefer not to say	3%
N/A	1%

Terminology

Due to the diverse descriptions of individual types of economic crime, the following categories were developed for the purposes of the survey.

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.

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.

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

Contacts

PwC Forensic Services

Ian Elliott
Partner, Leader of Government & Public
Sector Forensic Services Team
Tel: 020 7213 1640
Email: ian.elliott@uk.pwc.com

Andrew Gordon
Partner, Head of Investigations
Tel: 020 7804 4187
Email: andrew.gordon@uk.pwc.com

Kathryn Westmore
Forensic Services
Tel: 020 7213 2941
Email: kathryn.m.westmore@uk.pwc.com

