Navigating your way through stormy waters

A review of fraud risks in the public sector following the comprehensive spending review

Develop a risk resilient organisation pwc.co.uk/riskresilience
Fraud in a downturn

Contents

Introduction .................. 3

The perfect storm –
a heightened threat of fraud ............... 4

Emerging fraud risks –
what action can be taken? ............... 8

Conclusion ................... 15
Introduction

The current state of public finances has been well publicised with the budget confirming the coalition government’s intention to reduce public spending faster and more severely than under plans outlined by the previous government. Indeed, the budget revealed for the first time the austerity which lies ahead and confirmed the scale of the action proposed by the coalition government, representing the most significant public spending cuts since the Second World War.

The need for a reduction in government spending is generally accepted, although the severity of the reductions continues to cause significant debate and we are yet to see exactly how such cuts will be achieved. Given the current profile of public spending, and the announced ‘ring-fencing’ of certain areas, what is known is that there will be significant reductions in staffing costs, the termination of programmes, streamlining of systems and ceasing of activities in many areas of government.

Such changes will have a profound effect on public sector workers and private sector companies which rely on the public sector economy. When the prosperity of an individual or the survival of a company is jeopardised, our experience is that the line separating acceptable and unacceptable behaviour becomes blurred. When considered alongside the risk that opportunities to commit fraud will increase because of the expected changes in the machinery of government, resource limitations and diverted management focus, the likelihood of a significant increase in internal and external fraud against the public sector is a real threat.

The prospect of further losses, in addition to the estimated annual loss of £17.6bn\(^1\) experienced by the UK public sector economy as a result of fraud, is unacceptable, especially against the backdrop of a significant government deficit. PricewaterhouseCoopers\(^2\) believe that the losses attributed to public sector fraud should be seen as an opportunity to reduce the public sector deficit and identify funds for reinvestment.

In this paper we outline why there will be an increased threat of fraud in the future, where the growing threats exist and what mitigating actions could be taken to manage the risks.

---

1. Estimated public sector fraud loss in 2008, as published by the National Fraud Authority (March 2010).
2. “PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate legal entity.
The perfect storm – a heightened threat of fraud

The Fraud Triangle, developed by the criminologist Dr. Donald Cressey, describes three conditions that are commonly found when fraud occurs. The perpetrators experience some incentive or pressure to engage in misconduct. There must be an opportunity to commit fraud and the perpetrators are often able to rationalise or justify their actions.

The events that have led to the UK’s current financial position, and the coalition government’s proposed actions, have the potential to heighten significantly the risk of fraud as never before in the public sector. Our recent Fraud in the public sector report provided insight into the perceived impact that these three factors have on increasing the risk of fraud being committed:

- 71% of respondents attributed greater risk of fraud to increased ‘incentives or pressures’ – primarily as a result of employees’ fear of losing their job;
- 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.
Incentive/Pressure
While fraud can, from a legal perspective, be perpetrated by an organisation, the steps taken to commit fraud are always the actions of individuals. It is often assumed that people commit fraud for personal gain and in particular to obtain money. Whilst this can be true, the reality is far more complex. In the public sector, the avoidance of loss, whether it be future income or job security, is more likely to be the primary motivating factor. As people lose their jobs and those still in employment feel ever more threatened, the pressure and incentive to commit fraud will increase.

It is clear that government spending cuts will exert significant pressure on individuals within government. The prospect of unemployment is a real threat for thousands of public sector workers. The pressure on individuals in the public sector will be more intense than that experienced by private sector employees in the recent economic downturn, given the mindset that many long term public sector employees hold that a job in government is a ‘job for life’ – this is no longer the case. The real threat to the livelihood of thousands of individuals has significantly increased the incentive for individuals to act dishonestly.

In addition to the threat of job losses, public sector workers are also experiencing pressure on their personal finances due to the two year public sector pay freeze, ongoing speculation regarding pension provision and anticipated changes to redundancy packages.

The government’s intentions to restrict expenditure will also have a considerable impact on private sector businesses that rely on the public sector economy. We have already seen evidence within the private sector of companies feeling the effects of public sector contracts being withdrawn. When someone’s livelihood is at stake or the future of a company rests on obtaining a new order from the government, some people will more acutely feel the pressure to do the wrong thing: to pay the bribe that secures the company’s financial future or to look the other way while others do so. Such actions are unlikely to be limited to traditional fraudulent activity, such as asset misappropriation, but may come to light in areas such as performance misreporting, contract manipulation or bribery and corruption.

“As people lose their jobs and those still in employment feel ever more threatened, the pressure and incentive to commit fraud will increase.”
Opportunity
Change presents opportunity – significant structural and organisational change across government is guaranteed in the foreseeable future. Whilst change is not unusual, the expected magnitude and pace of change will have never been experienced before and it is this magnitude and pace of change which will generate significant opportunities to perpetrate fraud.

The coalition government’s interim announcements are leading to significant changes in the operations of government departments. For example, there have been several announcements proposing the closure of quangos and arms length bodies across government. More radical structural change is expected which will affect the core responsibilities of government departments. We have already seen that the proposed restructuring of the NHS is leading to concern over the robustness of contract scrutiny and management. To mitigate the heightened risk of fraud as a result of these changes, rigorous fraud prevention mechanisms should be incorporated as new systems and policies are developed, however, the pace of change and reduction in available resources to implement and manage the proposed changes present a real threat to this ideal.

Changes are not only expected at a structural level but the requirement to reduce costs will inevitably result in changes at an operational level through reduced resources, streamlining of systems and the removal of perceived ‘non value-add’ activities. For example, internal audit departments within government typically hold the responsibility for leading the fraud agenda in developing and championing prevention strategies as well as fraud detection and investigation. Not only are internal audit departments having to identify savings, but they are being asked to undertake a wider remit; for example, as consultancy support is reduced and gaps in project support and assurance begin to appear on major department programmes, internal audit are asked to fill the gap. The combination of fewer resources and a wider remit will result in internal audit departments becoming stretched, inevitably leading to a reduced focus on fraud prevention and detection.

In our experience, there are two key controls in preventing and detecting frauds – segregation of duties and reconciliations. As finance departments look to cut costs and reduce resources, there is a very real danger that these controls will be compromised, leaving the organisation vulnerable to attack.

Our overall concern is the pace of change and that the overwhelming focus on cost reduction will result in internal control systems being inadvertently weakened, further increasing the opportunities for fraudsters.
Rationalisation

The third element of the fraud triangle is the ability of individuals, be they front line staff or senior management, to rationalise a fraudulent act. There is a growing sense of resentment amongst public sector employees that they are paying the price for the mistakes that have been made in the private sector. This resentment will heighten the ability of individuals to rationalise fraudulent acts. Examples of rationalisation ‘logic’ we have experienced, with a particular emphasis on themes that will become more common as government cuts take hold, are included below:

“If the city bankers can keep their million dollar bonuses, why can’t I have a piece of the action?”

“Creative reporting’ is not fraud, it is just bending the rules.”

“I was entitled to a pay rise, so made up a bit of the difference via expense claims.”
We have outlined why the risk of fraud will be significantly heightened in the coming months, but where will the heightened risk of fraud emerge? There are many areas of fraud which may increase as a result of the changes being experienced, including misreporting, accounting fraud and third party fraud, such as benefit fraud. This paper focuses on several different types of fraud that we believe may increase along with suggestions for mitigating the risk.

The National Fraud Authority’s (NFA) recent publication *A fresh approach to combating fraud in the public sector* highlighted that staff and procurement costs account for 25% and 29% respectively of Total Managed Expenditure (TME) by the public sector. Given the size of expenditure in these areas, and the catalysts fuelling the increasing risk of fraud, we believe that staff and procurement fraud will represent significant areas of risk in the future. In addition, there are areas of fraudulent behaviour such as the manipulation of data (both financial and non-financial) to meet targets and data theft which should be of increasing concern to public sector organisations.

Many commentators on fraud describe how a particular solution is key to the management of fraud risk, be it ‘risk identification’, the ‘tone from the top’ or ‘better use of technology’. It is our belief that with all aspects of fraud a holistic response is required – there is no silver bullet that will provide a solution; rather a comprehensive framework is required to combat fraud successfully. The PwC Fraud Wheel\(^1\) sets out a comprehensive approach when addressing all fraud risks.

---

1. In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organisations measure the effectiveness of their systems of internal control. We have adapted the COSO framework to illustrate some of the key elements of a fraud and integrity risk control framework.
Staff fraud

The threat of fraud from ‘insiders’ has previously been considered low by the public sector and our recent *Fraud in the public sector* report indicated that only 39% of fraud cases reported by UK public sector bodies were committed by internal staff. This is in contrast to the private sector who reported that 56% of fraud was committed by internal fraudsters.

As the pressure on staff intensifies in the coming months, and the resentment of the changes being initiated in government grows, the likelihood of increased experiences of ‘insider’ fraud will rise.

Organisations must determine how best to implement a fraud risk strategy that will work for them, but in our experience there are a number of critical actions that continue to be under-utilised within many parts of the public sector in relation to staff fraud. Below are four potential solutions to consider.

1. **Staff risk assessment** – A significant emphasis within fraud risk management strategies is rightly placed on completing fraud risk assessments, allowing organisations to direct their resources most effectively to mitigate the risk of fraud.

   Opportunities exist within organisations to extend this approach and utilise such techniques in mitigating staff fraud. Government departments, and external agencies, hold a significant level of intelligence that would allow more effective fraud prevention and detection strategies to be developed; for example, through the categorisation and development of staff ‘risk’ profiles. Organisations should categorise the risk of staff fraud being committed using profiling techniques including area of work, access to finance systems, access to payment transaction and interactions with suppliers.

   The government has announced plans to use credit reference agencies to help detect benefit fraud. More controversial topics for further consideration include opportunities to extend this concept into areas such as the continuous monitoring of staff. Some advocates argue that the use of credit reference agencies could be very effective if used to highlight individuals who are experiencing financial difficulties, hence providing an opportunity for employers to provide support and mitigate any risk of fraud being committed. Whilst this approach would require amendment to existing data protection legislation, it could prove a very powerful tool to help organisations tackle staff fraud.

2. **Communication and training** – The benefits of proactive communication of, and training in, anti-fraud messages are well known. Our experience has shown that significant opportunities continue to exist within the public sector to communicate the institutional damage that fraud causes, the consequences for the individual and the opportunities that exist to improve the cost effectiveness of government organisations by reducing fraudulent activity. A small investment in training often reaps substantial rewards in reducing losses due to fraud.

   In addition to improved communication initiatives, opportunities exist to empower staff to be more effective in identifying fraud and integrity risks, and promoting the message that fraud is not acceptable. Operational and finance staff should be the first line of defence against fraud and integrity risks, however unless proper training on ‘business ethics’ is provided, this potential deterrent is lost.

Are you effectively managing your risk? 9
3. **Hiring and promotion** – Pre-employment screening is critical and is the first line of defence for all organisations. However, in the current economic environment – where there are likely to be significant job losses rather than recruitment – this element of an organisation’s strategy clearly becomes less significant. Nevertheless, ineffective pre-employment screening continues to be highlighted as a weakness in many cases of employee fraud or under-performance. It is also crucial that public sector bodies ensure that any companies to whom they outsource work have sufficient checks in place to prevent the organisation from becoming compromised.

4. **Whistle-blowing** – Intrinsically linked to the empowerment of staff and third parties, is an individual’s ability to ‘flag’ potentially fraudulent activity or highlight potential risks with confidence. The quality of whistleblower hotlines is highly variable across government departments, with weaknesses ranging from limited publicity of their existence, to a lack of confidence in the hotline processes that are established and the belief that the organisation does not have a ‘zero-tolerance’ approach to fraud. Our research has shown that whistleblowing procedures detect less fraud in the public sector than the private sector. Refreshing publicity with a focus on reporting suspicious activity as it relates to fraud will help to uncover otherwise invisible instances of economic crime.

A potential solution would be the implementation of an external whistleblower hotline that was used by all government departments – essentially a shared service solution. This approach would immediately provide the independent and confidential service which many employees perceive is presently absent. It would also present an opportunity to achieve cost efficiencies in the provision of this critical service.

The establishment of such a service could also be made available to third parties, including members of the public, hence providing a further route to ‘flag’ potentially fraudulent activity, such as benefits fraud, within government.

These four areas represent some of the opportunities that exist to empower public sector employees to support the government in mitigating the risk of insider fraud. Employees are invariably best placed to understand weaknesses in established systems and where opportunities to commit fraud exist. Employees are also best placed to understand the motivations and ethics of colleagues, and influence colleagues to raise the standard of integrity and ethics throughout the public sector. As government spending decisions begin to have an impact on employees, a real opportunity exists to engage with public sector workers on the issue of fraud and to reinforce the fact that allowing fraud to continue represents a genuine threat to their job security and ability to deliver excellent public services.
Procurement fraud

Our Fraud in the public sector report highlighted that procurement fraud is already pervasive within the UK. 77% of UK organisations that were victims of economic crime reported falling prey to asset misappropriation which frequently manifests itself as procurement fraud. Our Fraud in the public sector report also highlighted that of those respondents who suffered asset misappropriation in the last 12 months, 71% think it is likely that they will experience it again in the next 12 months.

Not only is procurement fraud likely to increase, it is often undetected for long periods of time. The typical procurement fraud lasts two years before it is detected. The impact of such a fraud can be severe and financial loss is often the least damaging aspect, as reputation, employee morale and business and regulator relations are all at risk.

Historically, the methods for proactively detecting procurement fraud have been limited to generic fraud prevention techniques and basic sample based testing of data, seeking to identify suspicious transactions (red-flags) through rules-based testing. Classic examples include round-sum invoices and late-night postings. The challenge is that these traditional red-flags are often not unusual events, and therefore the outputs from the tests are long lists of exceptions with many ‘false-positives’, leading to a high cost of manual investigation. Additionally, red-flag tests are well known and so are avoided by all but the most careless fraudster. The result is that proactive procurement fraud has frequently been perceived to be of limited value by management. A new, more intelligent and cost effective approach is required.

A fresh approach to fraud detection

In our experience the underlying methods of how procurement frauds are committed have not changed. Even with secure finance systems, fraudsters continue to find ways to circumvent controls and exploit weaknesses. Our experience demonstrates that procurement frauds are found to broadly align to eight types of scheme.

After investigating many procurement frauds, experience has taught us that each procurement fraud scheme leaves a typical ‘data fingerprint’. For example, a ‘kickback’ scheme will typically involve a large supplier, with purchase orders raised by a limited number of individuals and supplier relationships controlled by the same group of individuals.

Procurement fraud schemes

<table>
<thead>
<tr>
<th>Invoicing frauds</th>
<th>Conflicts of interest</th>
<th>Bribery and corruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>False-invoicing via dummy suppliers</td>
<td>Purchase schemes: overbilling</td>
<td>Kickbacks</td>
</tr>
<tr>
<td>Pass through schemes</td>
<td>Sales schemes: write-offs</td>
<td></td>
</tr>
<tr>
<td>Rebates from non-accomplice suppliers</td>
<td>Personal purchases</td>
<td></td>
</tr>
<tr>
<td>Personal purchases</td>
<td></td>
<td>Suppression of rebates</td>
</tr>
</tbody>
</table>
Data analytics can be applied to look for and find hidden patterns in the data of financial systems, which may be indicative of potentially anomalous or fraudulent behaviour. By using advanced data analysis techniques, incorporating tools such as data visualisation and data clustering, an organisation is able to search for the typical ‘data fingerprint’ of each type of procurement fraud. This proactive analysis reveals potential supplier relationships that demonstrate all the key characteristics of each procurement fraud scheme – putting the organisation in an excellent position to identify and mitigate any potential schemes.

This approach can be used to investigate known or suspected cases of procurement fraud. However, we believe the greater benefits lie in utilising such techniques proactively to identify potential procurement fraud earlier, and reduce loss. The application of data analytics can also act as an effective deterrent against potential fraudsters. Further opportunities exist across the public sector to minimise losses as a result of procurement fraud through greater use of information sharing in this area and more disclosure of identified procurement fraud schemes. This would provide a number of opportunities to improve prevention and detection success in this area including for example, blacklisting of identified offenders, sharing of new schemes to monitor and greater use of existing legislative powers to put greater emphasis on suppliers to improve controls in this area.
Manipulation of data

Fraudulent behaviour extends beyond asset misappropriation and procurement fraud. Our experience shows that manipulating data to meet both financial and non-financial targets is on the rise in public sector organisations. Numerous instances of ‘non-financial’ fraud involving the deliberate misrepresentation of disclosed information have been seen, for example in non-financial performance data. Water and electricity utilities have become embroiled in cases of this kind in recent years, whereby allegedly misleading data has been provided to the relevant regulators. There have also been examples of the deliberate misstatement of waiting list and other target data within the health sector.

Government departments are coming under increased pressure to meet targets with a reduced budget and limited resources. As a result, employees may be tempted to manipulate the figures to cover up gaps in performance. The widespread practice of this type of fraudulent behaviour undermines management’s efforts to promote ethical values throughout an organisation and creates a culture where unethical behaviour is allowed to flourish.

37% of individuals who believed that there were greater pressures to commit economic crimes in the current environment were concerned that targets would be more difficult to achieve. With fewer resources, this pressure will increase. Some organisations and particular employees are also able to rationalise the misstatement of data – often this type of behaviour is seen as harmless ‘poetic licence’ to achieve a particular objective rather than fraud on taxpayers or service users.

Organisations must ensure that they are monitoring the performance of individuals and are able to identify when staff might feel under particular pressure. It is also important that information is triangulated so that senior management see the ‘full picture’ and identify any inconsistencies in reporting.

A well-known public sector organisation was required to report its measures of success to the regulator. A whistleblower alerted the regulator to irregularities in the measurement process exposing the organisation to large fines. The organisation had to work closely with the regulator to demonstrate that it had the procedures in place to ensure the accuracy of the information and that remediation action had been taken to address the gaps in their controls.
Loss of data

In the past, discussions about fraud, integrity and asset losses have tended to focus on cash, tangible assets and financial securities, however in recent years the issue of data loss has been high on the agenda. In 2007 and 2008, the losses of personal data experienced by Her Majesty’s Revenue and Customs along with other organisations were widely reported and public concern about the amount of information held by government departments has increased.

21% of respondents in our recent survey on Fraud in the public sector considered that their organisation was likely to experience intellectual property infringement, including loss of data, in the next 12 months although just 6% had experienced it in the last year. This response reflects a growing awareness and concern about the safety of data held by government departments.

To date, most serious losses of personal data appear to be the result of mishap, not serious fraud or misconduct, although there have been some exceptions. The nature and extent of the data about people that government organisations hold makes them a key target for fraudsters. Departments including the DWP and HMRC have been targeted in recent years because of the volume of information held about members of the public, but other public sector bodies must be alive to the risk.

The threat of data loss often arises because of the inadequacy of controls. In our experience, many organisations have begun to put arrangements in place to improve data security. However, not enough is being done to address the risk of deliberate theft by criminal organisations working in collusion with permanent, short term or temporary staff to infiltrate organisations and circumvent existing control systems.

A key element in the fight against organised crime is for organisations to know their employees. The steps set out in this paper will not only help to mitigate staff fraud but will help to protect departments against theft of data by individuals.
The coalition government’s approach to reducing the public sector deficit has initiated a new era of public policy which will result in significantly reduced public spending. It is widely accepted that there will be significant reductions in staffing costs, capital programmes and the streamlining of systems to achieve the reductions being proposed. In addition to the size of the reductions expected, the coalition government has also made a clear statement of intent that any reductions will be fast tracked, wherever possible, to achieve swifter reductions than had been planned by the previous government.

The magnitude and speed of the proposed changes will have a profound effect on public sector workers, as well as private sector companies that rely on the public sector economy. The increased pressure on individuals’ prosperity through job insecurity and pay freezes, coupled with the likelihood that opportunities to commit fraud will increase, creates a ‘perfect storm’ resulting in a heightened fraud risk from within and from associated third parties.

In the current climate, the two key areas of significant risk to organisations are staff fraud and procurement fraud and a comprehensive framework is required to address these risks. It is also vital that public sector organisations consider the use of data analytics and staff risk assessments to identify possible areas of concern. However, fraudulent behaviour extends beyond asset misappropriation and procurement fraud and both the misreporting and the theft of data can have damaging consequences on an organisation’s finances and reputation.

This heightened fraud risk comes at a time when there is a real opportunity for the coalition government to reduce fraud and restrict the current estimated annual losses of £17.6bn experienced by the UK public sector economy as a result of fraud.

Current practice in combating fraud within the public sector is improving and there are examples of excellent initiatives being employed to minimise the current losses, particularly around benefit fraud. However, there remains an opportunity to achieve greater consistency in approach across all government departments and employ new approaches to minimising fraud, for example through the use of more advanced data analytics. The good news is that effective fraud risk management more than pays for itself. Attacking fraud, waste and abuse offers a huge cost savings opportunity for a relatively low investment.

We believe that the potential reduction in significant losses due to fraud should be seen as an opportunity to reduce the public sector deficit and identify funds for reinvestment.

“The increased pressure on individuals’ prosperity through job insecurity and pay freezes, coupled with the likelihood that opportunities to commit fraud will increase, creates a ‘perfect storm’ resulting in a heightened fraud risk from within and from associated third parties”
About Forensic Services
The Forensic Services group of the PricewaterhouseCoopers global network of firms plays a lead role in addressing the lifecycle of fraud and other avoidable losses, providing reactive investigative services and proactive remedial and compliance services to clients in the private and public sectors.

The UK team comprises over 250 dedicated partners and staff who specialise in areas such as investigations, fraud risk management, avoidable loss identification & mitigation, cost control, anti-money laundering, anti-bribery & corruption and corporate intelligence. The Forensic Services practice is supported by a team of forensic technologists who provide data mining and electronic discovery type services.

About the authors
**Ian Elliott** is a partner in the Forensic Services group at PricewaterhouseCoopers LLP (UK). He leads the Government and Public Sector team, specialising in the investigation of complex fraud, regulatory and integrity issues.

ian.elliott@uk.pwc.com
+44 (0) 20 7213 1640

**Andrew Gordon** is a partner in the Forensic Services group at PricewaterhouseCoopers LLP (UK) and leads the Investigations practice in the UK. Andrew is experienced in the investigation and remediation of a wide range of large, complex matters involving fraud, corruption and other misconduct.

andrew.r.gordon@uk.pwc.com
+44 (0) 20 7804 4187