Tackling fraud effectively in central government departments

Gilbert, Michael and Wakefield, Alison ORCID logoORCID: https://orcid.org/0000-0002-1553-9178 (2018) Tackling fraud effectively in central government departments. Journal of Financial Crime, 25 (2). pp. 384-399. ISSN 1359-0790

http://dx.doi.org/10.1108/jfc-01-2017-0006

Title:

Tackling fraud effectively in central government departments:

A review of the legal powers, skills and regulatory environment of UK central government counter fraud champions

Alison Wakefield and M. Gilbert

Abstract

Fraud has a significant effect on society. It has been estimated to cost the UK economy more than £50 billion annually (National Fraud Authority (NFA), 2013, p.2) and the Government has signalled its determination to tackle these losses through a range of preventative, enforcement and collaborative activities. Diminishing police resources allocated to fraud mean that this activity will need to be delivered by both law enforcement and civilian counter fraud teams (Attorney General's Office (AGO), 2006, pp.128-129; Cabinet Office & NFA, 2011a, 2011b, 2011c).

This research sought to establish whether UK central government organisations have the legal powers, skills and regulation needed to tackle fraud effectively. It was concluded from the literature review that an effective legal framework, supported by a wide range of skills, is essential to the delivery of the UK government's zero tolerance approach, and that both professional standards, and the civil rights of those subject to investigation, should be protected through some form of regulation. Empirical data, collected via a questionnaire and a semi-structured interview programme, suggested that the effectiveness of central government civilian counter fraud teams is hampered by a fragmented legal landscape and a lack of skills, and that further professionalisation and regulation is needed to protect professional standards and individual legal rights.

Key words: counter-fraud, fraud, legal powers, professionalism, regulation, training

Journal Article

Introduction

Fraud is estimated to cost the UK economy £52 billion annually, of which £20 billion is seen to relate to the public sector (NFA, 2013, p. 2). In 2011, the UK Government published its strategy to tackle fraud in two principal documents – '*Eliminating Public Sector Fraud'* and '*Fighting Fraud Together*' (Cabinet Office and NFA, 2011a, 2011b). Both documents signalled an intention to decrease the losses to the UK economy due to fraud – and in particular, the £20 billion lost to the UK public sector in both 2011 and 2012 (NFA, 2012, p. 7; 2013, p. 2). Both documents place a significant emphasis on fraud awareness and prevention, as recommended by the Fraud Review Final Report published in July 2006 (AGO, 2006, pp. 8, 116). Both also emphasise the need for improved information on fraud whether this be improved intelligence on fraudster behaviour and activity (*Fighting Fraud Together*) or in the risks and threats faced by individual organisations (*Eliminating Public Sector Fraud*).

'*Eliminating Public Sector Fraud*' also emphasised the need for a collaborative response to implementing a zero tolerance approach to fraud, while '*Fighting Fraud Together*' stressed the need for more effective enforcement activity to detect those committing fraud and ensure that they receive appropriate sanctions. Limitations on police resources mean that this approach will need to be delivered by both law enforcement and civilian counter fraud teams and particularly as fraud is not a policing priority (Home Office, 2004; Gannon and Doig, 2010, p39). Each major central government body is required to have a counter fraud champion to improve knowledge of fraud against Government departments (Cabinet Office and NFA, 2011b, p. 16).

The collaborative working envisaged by the Cabinet Office presents a number of practical challenges. The activities of many public sector bodies are principally governed by their enabling legislation, the common law or the Royal Prerogative (Department for Constitutional Affairs 2003). Differing legal frameworks can lead to both ineffectiveness and inefficiency when tackling fraud. Fisher, (2010, p.1), for example, posits that the present arrangements for fighting fraud in the UK's financial markets 'are lamentably deficient'. One of the reasons for this is that, the bodies concerned operate under different statutory frameworks which leads to “overlapping responsibilities and an unnecessary duplication of both manpower and specialist resources”.

Convergence in legal frameworks and powers is insufficient in itself to ensure effective counter fraud management. Fraud management needs skilled staff with knowledge of the law, investigative techniques, the ability to manage evidence and exhibits and take witness statements and the capability to provide interview transcripts and surveillance evidence. It also requires a high degree of inter-personal and interviewing skills (Button, Johnston and Frimpong, 2008, p. 245). In addition, fraud investigations need access to specialist skills such as accounting and computer forensics, and especially the latter, as more and more information is held in electronic rather than paper format. Similarly, fraud prevention needs staff skilled in system design and control, so that appropriate action can be taken to identify and counter potential threats and control weaknesses which could lead to theft, data loss or corrupt activity (Krambia-Kapardis, 2002, p. 245).

It appears that staff qualified in these areas are thinly spread. The reasons for this are complex. Research by Frimpong and Baker (2007, p. 132) suggests that this may be due to the low status afforded to counter fraud staff, a lack of resources, inadequate training, poor pay, poor career prospects, management apathy and out of date legislation.

However, the Cabinet Office proposals for tackling fraud in the UK public sector and economy only partially deal with these issues. While their proposals for eliminating public sector fraud refer to the need to train all staff and change organisational cultures there is no mention of the skills, training and retention issues for the front line staff who are to deliver these proposals. The same is true for their proposals for tackling fraud in the UK economy (Cabinet Office and NFA, 2011a, 2011b).

The Cabinet Office has alluded to the need for improved governance over counter fraud activities. To achieve this, it proposes that different organisations and sectors come together under some form of umbrella arrangements (Cabinet Office and NFA, 2011b, p. 22). However, it is silent on how those bodies that have legal powers to counter fraud should have their activities regulated – despite the fact that, in using these powers, civilian counter fraud bodies can cause harm. In one case, a fraud investigation against a professional, precipitated by a whistleblowing letter to the relevant counter fraud service, led to his business going into administration despite the judge halting the trial against him and stating, 'You leave [this courtroom] vindicated with your good name intact and your head held high' (Baker, 2011, p. 5). Regulation can also help to underpin professional standards and the quality of the investigative process.

In avoiding such regulation, civilian counter fraud teams within the public service are treated differently from the Police, the UK Border Force, the private security industry and HM Revenue and Customs each of whom are, or will be, subject to external regulation (IPCC, 2011; SIA, 2014). While professional bodies such as The Institute of Counter Fraud Specialists exist, membership is voluntary. The current situation makes the application of common standards difficult and holding individuals, teams and organisations to account for their actions, problematic.

The aim of the research presented in this article was to examine, through empirical research, the legal powers and skills available to UK central government counter fraud champions to manage their fraud risk effectively. It also considered whether, in exercising their powers, civilian counter fraud champions are subject to appropriate regulation and control.

Methodology

Empirical data was collected through a mixed methods approach. It involved a programme of semi-structured interviews with representatives from 26 different organisations who were placed in one of three groups (Table 1) and a postal survey of all 32 senior civil service counter fraud champions from which a 50 per cent response rate was obtained.

Figure 1: Interview summary

Group		**Number interviewed**
Group 1	Representatives from central government counter fraud teams.	11
Group 2	Representatives from the wider counter fraud community that included those working for regulators, law enforcement, academia and audit organisations.	8
Group 3	Representatives from policy organisations,	7

	professional institutes and professional bodies.	
Total		26

The questionnaires were distributed by e-mail, with the support of the responsible department, to the counter fraud champions with a covering letter. The survey was restricted to public sector counter fraud champions, whereas the interview programme represents a more wide-ranging and detailed review that included policy makers, regulators, academics and others who are one step removed from front line service delivery.

Research Findings

This research sought to shed more light on the issues surrounding the legal powers, skills and regulatory framework in place to deliver the Government's vision for tackling fraud in the UK central government sector. The implications of these findings are then applied to the Government's current enforcement policies and their zero tolerance approach in particular.

Legal Powers

Interviewees and survey respondents were asked about the legal powers available to them when conducting counter fraud work. These covered the authority to investigate, surveillance, information sharing, interviewing, the acquisition of evidence, arrest and detention, prosecution and redress.

Table 2 lists the responses given to questions about legal powers to investigate fraud. The responses are similar to those found by Fisher (2012) who posited that differing legal frameworks adversely affect the effective delivery of counter fraud services. This research showed, for example, that between one third and one half of the bodies indicated that they do not have the legal power to investigate fraud and, for those that do, their ability to investigate fraud is constrained.

Figure 2: Gap analysis of powers available to central government bodies				
No	**Question**	**DESIRED** (1)	**PERCEIVED**	**SURVEY 2012**
The power to investigate				
A.1	The power to conduct fraud and other investigations to the civil and criminal standard	100%	65%	50%
The power to conduct surveillance				
A.2	The power to conduct directed Surveillance with and without RIPA registration	80%	61%	25%
A.3	The power to monitor staff e-mails and phone calls while working in official premises	100%	100%	63%
A.4	The power to monitor contractor e-mails and phone calls while working on official premises with or without a warrant or RIPA registration	96%	91%	38%
The power to obtain and share information				
A.5	The power to issue third parties with a notice under s29 (3) of the Data Protection Act 1998 when seeking information in a fraud or corruption enquiry	100%	83%	38%
A.6	The power to share data with law enforcement and private sector security and civilian counter fraud teams	100%	87%	68%
The Power to Interview				
A.7	The power to interview and take witness statements	100%	96%	75%
A.8	The power to interview under caution	80%	74%	19%
A.9	The power to compel staff, contractors and other individuals to attend for interview with self incrimination safeguards	80%	48%	19%
A.10	The power to compel staff, contractors and other individuals to attend for interview without self incrimination safeguards	32%	22%	6%
The Power to Obtain Evidence				
A.11	The power to obtain a search and seize warrant	68%	22%	0%
A.12	The power to obtain production / other information gathering orders	88%	43%	0%
A.13	The power to obtain and review financial and finance related documents	88%	43%	38%
A.14	The power to enter third party premises (e.g. contractor Head Office, Personal Homes) to seize documents, computers and other evidential material with a warrant	60%	26%	0%
A.15	The power to receive information and / or documents and / or evidence from a source when permission from the document / evidence owners has not been granted	76%	22%	31%
A.16	The power to compel staff and third parties (e.g. contractors) to supply documents and other required evidence with self incrimination safeguards	76%	30%	13%
A.17	The power to compel staff and third parties (e.g. contractors) to supply documents and other required evidence without self incrimination safeguards	32%	9%	6%
A.18	The power to search an individual while on official premises	72%	35%	25%
A.19	The power to search an employee's desk, locker, work bin etc. within official premises without a warrant / other court order	96%	87%	56%
A.20	The power to search a contractor's desk, locker, work bin etc. within official premises without a warrant / other court order	92%	83%	50%
A.21	The power to forensically examine and copy an employees work computer without a warrant / other court order	100%	96%	69%
A.22	The power to forensically examine and copy a contractor's computer system without a warrant / other counter order	88%	78%	6%
The Power to Apprehend and Detain				
A.23	The power to arrest an individual when suspected of fraud and / or corruption against your organisation	16%	4%	0%
The Power to Prosecute				
A.24	The ability to bring prosecutions in the organisation's own right for fraud and corruption cases – rather than through law enforcement and the CPS	72%	35%	6%
The Power to Obtain Redress				
A.25	The power to issue a formal caution	60%	17%	6%
A.26	The power to make a compensation claim under the civil law for losses suffered	92%	78%	50%
A.27	The power to make a compensation claim under the criminal law for losses suffered	88%	78%	19%
A.28	The power to recover sums paid in salary and other benefits, while employed or on suspension, if the case against the accused is proven (2)	84%	61%	13%
A.29	The power to recover investigation costs (2)	84%	26%	13%
A.30	The power to issue an administrative penalty	72%	17%	31%
Note (1): One interviewee declined to offer an opinion on the powers that civilian counter fraud teams should have.				
Note (2) These items were included as one power for the survey. However, following further research, it was decided to split these into two separate powers for the interview programme as they represent recoveries from two distinct areas of recoverable expenditure.				

In addition, representatives from some organisations reported that they did not have the power to monitor employee e-mails and other communications, while a quarter of survey respondents stated that they were unable to conduct interviews or take witness statements. Less than one half of interviewees, and no survey respondents, believed they could obtain warrants or production orders to obtain information or enter third party premises. Similarly, less than one half of all interviewees, and less than a quarter of survey respondents, considered that they could compel staff and third parties to attend for interview. However, the perceived ability to obtain and review finance and financial related documentation was similar between the two populations at around 40 per cent of respondents. Conversely, there was a difference between the two populations over data sharing. While 83 per cent of interviewees considered that they could request information under section 29 of the Data Protection Act 1998 this figure fell to 38 per cent of survey respondents.

These findings show that many central government bodies may be severely constrained in their ability to obtain the information needed to investigate fraud and corruption, and particularly as: only around two thirds of interviewees and one quarter of survey respondents can search an official while on their premises; some interviewees and survey respondents report that they cannot search their staffs' lockers and desks, or forensically analyse an employee's computer; and one quarter of interviewees and four fifths of survey respondents report that they cannot interview under caution. This further suggests that central government bodies may struggle to fill the gap caused by a lack of law enforcement capacity to tackle financial crime (Gannon and Doig, 2010, pp. 40, 50-51). It also casts doubts on whether they can provide the complementary policing resource envisaged by the Fraud Review Final Report (AGO, 2006, pp. 9-10).

Table 3 summarises responses from interviewees who considered that a lack of powers was having a deleterious effect on their ability to manage fraud. These have been grouped into the following categories: Policy and Strategy Formulation; Risk Management, Detection, Investigation, Sanctions; Deterrence and Prevention. It shows that all major aspects of fraud management are affected.

While investigation was seen to be the most affected area, as expected, the most significant effect according to interviewees lay in its impact on policy and strategy formulation. Their accounts suggested that, by inhibiting their understanding of how and why fraud is committed, it is more difficult for those managing fraud in these organisations to identify what constitutes a proportionate response, and justify appropriate levels of investment, as the full extent of the fraud problem may be understated.

Figure 3: Identified effect of a lack of legal powers
Policy and Strategy Formation
It inhibits an understanding of how and why fraud is committed
Risk Management
It inhibits the development of business centred fraud typologies
It impacts on the development of fraud risk assessments
Detection
It inhibits an understanding of how to tackle fraudster methods
It inhibits proactive fraud detection
Investigations
It makes it difficult to apply a public interest test
Easier investigations will be cherry picked which reduces recoveries and fraud prevention
A sub-optimal number of investigations are undertaken
It affects consistency of treatment when allegations are received
It impacts on evidence collection
It causes difficulties in referring cases to law enforcement as the evidence needed cannot be collected
Frauds go uninvestigated as the police are reluctant to become involved
Sanctions
It has a deleterious effect on the administration of justice
It affects the ability to levy effective sanctions and penalties
Deterrence
There is a lack of an effective visible response
It impacts on deterrence and prevention
It undermines counter fraud control systems / structures and detection mechanisms
Prevention
It is difficult to prove non-compliance with internal policies etc.
It limits data sharing opportunities

Figure 1 lists the possible solutions proposed by interviewees to close the legislative gap. This shows that thirteen interviewees noted that additional legislation would be required to provide them with additional powers. However, this was not seen as the only solution. 12 interviewees observed that, in the new operating environment with more third party outsourcing, it is essential that relevant access clauses be built into supplier contracts. A further two participants noted that such access clauses should also be extended to grant agreements.

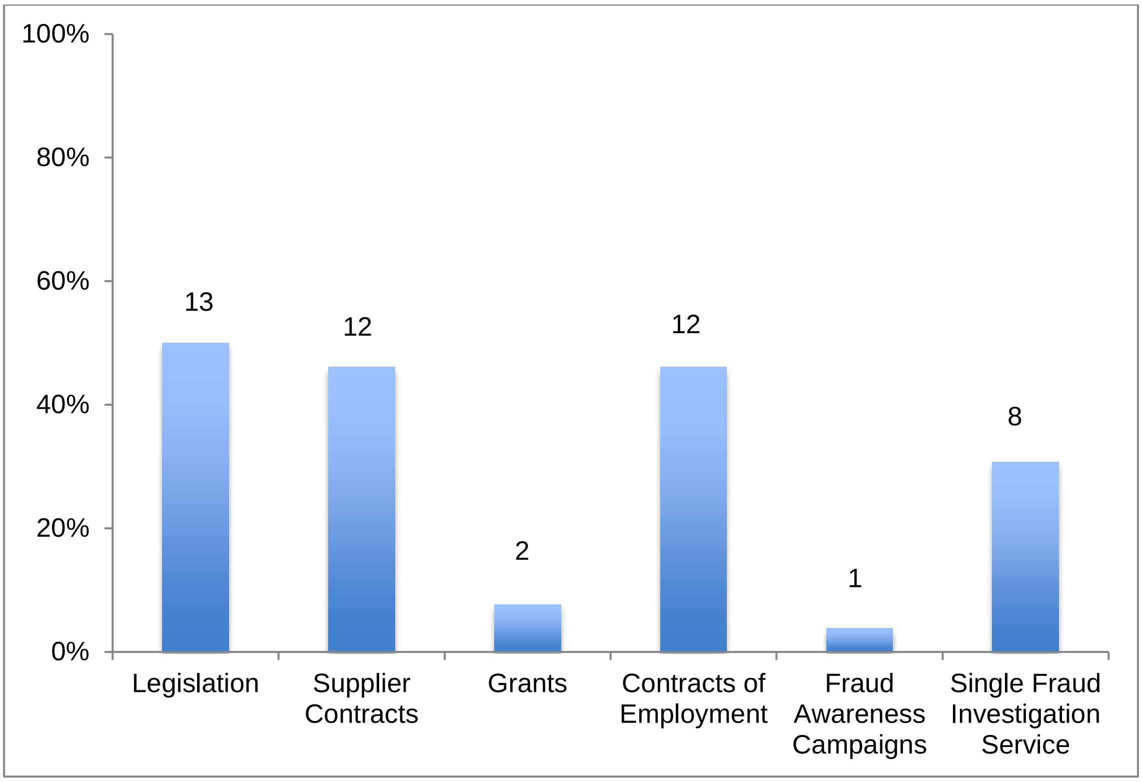

Figure 4:Methods for dealing with a shortage of legal powers

Similarly, for staff, 12 interviewees from all three groups observed that it is also important to allow for appropriate investigative techniques to be built into contracts of employment. Such clauses, it was posited, set out clear expectations and, in doing so, help enforce fraud deterrence. These participants noted, however, that there could be difficulties in enforcing such contracts. In addition, one interviewee noted that they rely on implied legal powers to protect their services, assets and finances from fraud. Another observed that:

> The first step is to ensure that counter fraud receives professional recognition – to give others confidence that fraud investigators will use any powers given to them responsibly and proportionately within some form of regulatory framework through which they are held to account.

Once this was in place, it was argued, further legislation could be considered.

Counter Fraud Skills

A similar picture emerges for available counter fraud skills. The research showed that, even if central government bodies had the legal powers needed to combat fraud effectively, they may struggle to use them successfully. Of the bodies surveyed, 7/16 had no Accredited Counter Fraud Specialists (ACFS) and only 2/16 had qualified Association of Certified Counter Fraud Specialist staff. Only 8/16 had staff with accountancy or internal audit qualifications and only 1/16 surveyed organisations had a staff member trained in computer forensics or Proceeds of Crime Act (POCA) 2002 recoveries. Finally, 3/16 relied on internal audit to provide one or more of the skills needed.

Evidence from interviewees may explain this position. Only five interviewees (20 per cent) reported that their organisations had carried out some form of counter fraud competencies assessment, of which only one worked for a counter fraud team, and only five had some form of training plan. Interviewees also put forward organisational reasons for the absence of a competency analysis. The scale of the competencies needed to implement the fraud management model is such that skilled resources are bought in when needed; counter fraud awareness, prevention and activities are seen as stifling innovation; and fraud is not seen as a major organisational problem that needs an expensively trained resource to tackle. For example, one counter fraud practitioner observed that:

> The appetite for fraud awareness, identification and prevention has yet to be fully defined. This is because such activities are seen as a stumbling block to progression of new and innovative services.

Interviewees from all 26 organisations were asked to list their top ten core skills and competencies and, between them, identified 66 different skills and competencies that, in their view, need to be employed to deliver an effective counter fraud service. To help draw out key themes each competency has been grouped into one of four categories: innate skills; technical skills; organisational skills; and professional skills. These categories have been designed to reflect the different ways people learn and acquire knowledge. Innate skills are acquired by individuals over a long period of time and are often recruited into the business and continually developed. Technical skills can be acquired through appropriate training courses, and if supported by adequate levels of practical experience, can be learned fairly quickly. Organisational skills relate to a particular organisation and are acquired through in-house courses and work experience, are often specific to the employer and form an integral part of service development. Finally, professional skills are often externally determined, learned through a period of study, and require technical experience to discharge effectively.

Many settled on identical and similar competencies and skills, suggesting that there is a common understanding of personal characteristics and knowledge needed to deliver an effective counter fraud service. Table 5 lists the top 25 competencies, according the number of interviewees who mentioned each of these, in their interview. Figure 3 summaries the number of skills placed in each of the four specified categories.

The most interesting aspect of interviewees' answers is the prevalence of innate skills in the list of the most popular 25 competencies. Given the importance of these personal qualities to counter fraud teams, it is surprising that some interviewees report that these are either absent or only partially developed in their staff. While interviewees from counter fraud teams stated that some of their staff lacked interpersonal, interviewing, technical and legal skills, all reported that their staff had well developed analytical skills. Such a view was not, however, shared by the organisations in the wider counter fraud community and policy and professional bodies groups. This suggests that there may be a divergence of internal and external views on the quality of some aspects of counter fraud work. This does not necessarily imply poor analytical skills. It may be due to an expectation gap and the way in which counter fraud teams are perceived when discharging their responsibilities.

Figure 5: 25 most commonly sought counter fraud competencies				
No	**Skill**	**Core?**	**%**	**Absent?**
	Innate Skills			
1	**Well developed analytical skills** Be able to work with, and analyse meaningfully, qualitative and quantitative data	23	88%	5
3	**Objectivity and independence** Work must be free from bias, reflect the facts and lead to balanced conclusions	17	65%	5
6	**Tenacity and resilience** Tactfully follow through all tasks to completion without being deflected by others	15	58%	2
7	**Influencing skills** Ability to present views to senior managers and represent organisation credibly	14	54%	8
11	**Judgement and proportionality** Recognise where fraud risk is in organisational priority and devise apt response	5	19%	0
12	**Honesty / integrity / impartiality** Evidence based work which from which personal bias is absent	5	19%	0
13	**Excellent written skills** The ability to write reports and other documents clearly, concisely & persuasively	5	19%	2
15	**Commitment to ethical values** All work must subscribe to the seven Nolan Principles of Public Life	4	15%	0
16	**Communication skills** Ability to bond effectively with all –e.g. managers, victims, witnesses & suspects	4	15%	1
19	**An enquiring mind and intensive critical thinking** Ability to know where fraud exposures are / will be and devise workable solutions	3	12%	0
20	**Innovative mind set** Ability to think of new ways to tackle both current and new issues	3	12%	2
21	**Adaptability** Ability to apply personal and professional skills to a variety of situations	3	12%	1
	Technical Skills			
2	**Interpersonal and interviewing skills** The ability to strike positive relationships with others and interview effectively	22	85%	6
5	**Technical and legal knowledge** The ability to progress tasks according to the law and best industry standards	17	65%	7
9	**Strong process mapping and analysis skills** Ability to document, analyse and assess systems and processes	8	31%	2
18	**Accuracy in record keeping and attention to detail** Keep meticulous and accurate file records and notes in a methodical manner	4	15%	0
24	**Ability to pull together and summarise evidence** Ability to present evidence in a logical, coherent, consistent and objective manner	3	12%	0
25	**Case building and management skills** Taking ownership of a case from start to finish which meets pre-set objectives	3	12%	1
	Organisational skills			
10	**Collaborative working** Ability to work in partnership with other internal and external departments / bodies	6	23%	3
14	**Awareness of legal and technical limitations** Knowing what is legally and technically allowed and remaining within these limits	5	19%	1
22	**Understanding data sources and applying detection techniques** Knowledge of MIS systems and how to interrogate these for anomalies	3	12%	1
23	**Knowledge of the fraud landscape** Knowledge of the organisation's business and likely fraud exposures	3	12%	1
	Professional Skills			
4	**Strong risk assessment and management skills** Ability to identify, assess and assist others to control fraud risks	17	65%	6
8	**Strategic assessment** Ability to see the big picture and draft strategies to deal with identified fraud risks	9	35%	7
17	**Well developed IT and cyber security skills** Understand IT fraud risks and the measures needed to detect and combat these	4	15%	2

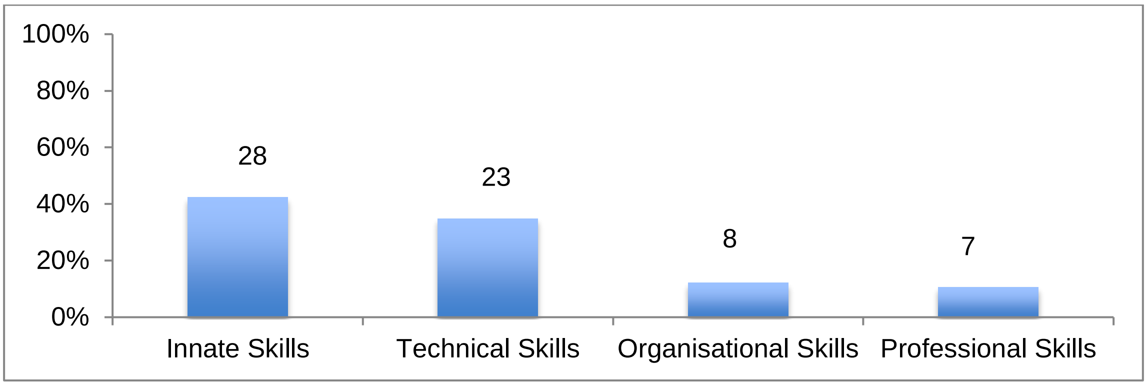

Figure 6: No of identified competencies by category

Those interviewees who placed importance on organisational skills report that key issues such as: knowledge of the fraud landscape; an awareness of legal and technical limitations; and an understanding the different data sources and being able to apply appropriate detection techniques to these, were largely being met. The issue of most concern was collaborative working where 50 per cent of interviewees, who saw this as a key skill, reported that their staff either fully or partly lacked this ability. This lack of collaborative working may extend to allied skill groups and partly explain why counter fraud managers are reporting a lack of access to professional skills such as strategic assessment, risk assessment and management and IT and cyber skills.

Figure 4 shows that most interviewees use a range of training methods that include external and internal training courses, desk training, mentoring, and continuous professional development (CPD).

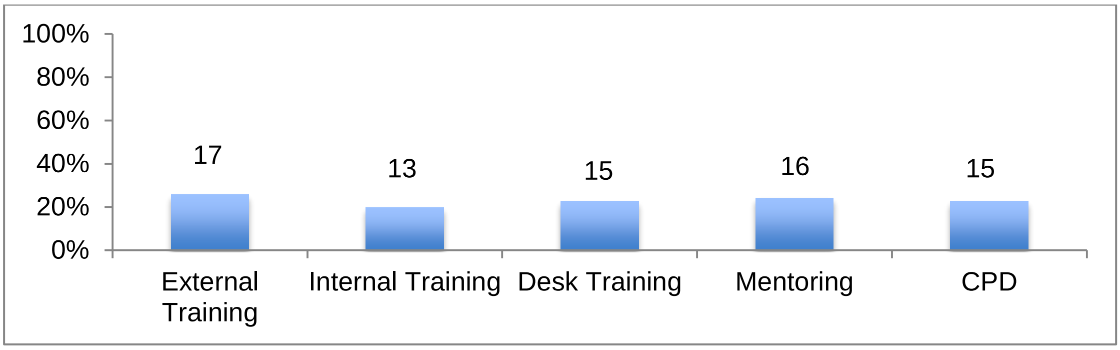

Figure 7: Training methods employed

Counter Fraud Regulation

Civilian counter fraud investigations can be intrusive and lead to harm (Phillips, 2012, p.77; Hurrell, 2014). This section therefore examines participants' attitudes to ways in which civilian counter fraud services within central government should be overseen and controlled to minimise this risk. It considers both self-regulation, in the form of internal management supervision over counter fraud operations, and whether some form of external regulation, such as state control, co-regulation (where occupational codes of conduct are given legislative authority) or enforced (or quasi) self-regulation might be appropriate (Australian government, 2007).

The decision on whether to regulate or not, and the choice of regulatory mechanism, is complex. Effective regulation can have a positive influence over service standards and individual and corporate behaviours and reduce costs (Samarajiva 2001; Wiig & Tharaldsen, 2007; Andrews et al., 2008; Gunningham & Sinclair, 2009). However, it can also have high compliance costs, lead to sub-optimal performance by regulatees due to inflexibility in regulatory processes and stifle innovation (Porket, 2003; Centre on Regulation and Competition, 2004; Australian government, 2007). In addition, regulation through external bodies, such as professional institutes, does not always guarantee appropriate behaviour in all circumstances (Snyder, 2014).

There was widespread support from interviewees for being subject to internal supervision with all 26 believing this to be necessary for the reasons given in Figure 5.

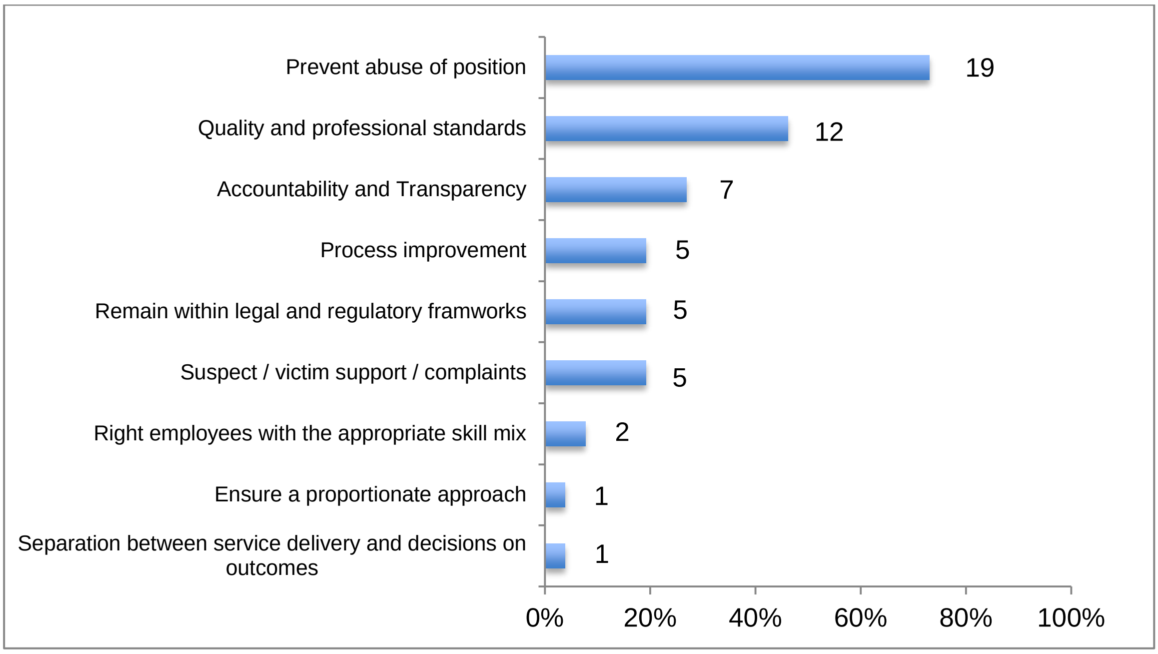

Figure 8: Principal reasons for the need for internal supervision

Furthermore, of the 14 survey recipients who expressed an opinion, eight (57 per cent) considered that the current regulatory arrangements were satisfactory and of the remaining six, five (83 per cent) were in favour of an approach based around self-regulation. Therefore, there appeared to be significant support for internal supervision within the central government counter fraud community.

Of the reasons provided in Figure 5, the most striking were the need to prevent an abuse of position; the development and maintenance of appropriate quality and professional standards; and having the right employees with the appropriate skill mix. These, coupled with the need to ensure that counter fraud teams remained within their legal and regulatory frameworks, suggest that the issues covered by this research resonate with others working in this field.

17 interviewees (65 per cent) were in favour, in principle, of some form of external regulation. One commented:

> Counter fraud teams need to be subject to scrutiny and oversight to prevent an abuse of the powers invested in them and to ensure that management, cost and performance pressures do not lead to serious issues being overlooked.

Other common reasons cited by interviewees for the need for some form of external regulation included the maintenance of quality and the prevention of poor and illegal practices (4 interviewees), and the provision of an externally validated framework that underpins independence (3 interviewees). One interviewee also noted that:

> Any team invested with formal powers to conduct investigations into others should be subject to scrutiny by a competent authority to ensure that these powers are used proportionately, appropriately and only when necessary.

Accountability and transparency were also issues raised by participants. One interviewee posited that increases in accountability and transparency in recent years had led to an improvement in public confidence in the police. Another considered that the need for transparency and accountability also extended to the civilian counter fraud teams. They noted that:

> Counter fraud staff must build and maintain public confidence – and this means transparency in the way they operate and clear accountability for their actions – which can, in extreme circumstances, lead to damage to their professional and personal life and ultimately, cause those found guilty of fraud to lose their liberty.

Redress for those who have suffered damage or loss following civilian counter fraud activities was also cited as a reason for some form of external regulation by nine interviewees drawn from all three groups. Another interviewee noted:

> There also need to be frameworks in place to allow those affected by investigations, or other counter fraud activities, to complain and for errant counter fraud professionals to be prevented from practising, where this is appropriate.

12 interviewees (46 per cent) from all three groups posited that the need for external regulation increased with the growth of legal powers. Thus, they believed that the larger the number of powers, and the greater the potential for intrusiveness, the greater the need for external regulation. 11 interviewees (42 per cent) from all three groups also observed that an anomaly exists at present whereby the way in which traditional law enforcement use their investigatory powers is externally regulated (for example by the IPCC), but civilian counter fraud professionals are not.

Nine interviewees (33 per cent), by contrast, were against the external regulation of counter fraud services. They cited three key reasons for this: a lack of investigative powers which meant that this level of external oversight was unnecessary; its predominant focus on internal matters, many of which end with disciplinary hearings and contract sanctions; and adequate levels of internal management oversight. One counter fraud practitioner went further, arguing that:

> Civilian counter fraud should be, and remain, business as usual for public administration. [They] noted that professional bodies already regulate many of the individuals who work in the counter fraud space. For example, many of those who work in the counter fraud already belong to accountancy or internal audit institutes.

Another interviewee concluded that a resolution to the regulation issue was for a convincing case to be made for it. They saw this as being the need for a professional and effective service to counter the £20 billion lost to fraud [by the public sector] annually and to underpin effective governance and financial regulation. They also observed:

> With frauds now spanning both private and public sectors (as private companies provide services to departments), there is a need for a central regulator to span all counter fraud operations that should be financed accordingly.

Research results demonstrate that the choice of regulatory regime is complex. One interviewee posited that, of the four main options, regulation by government, profession, organisation or self-regulation, counter fraud teams would prefer the fourth option. In their view it was the:

> Easiest and cheapest to implement and gives teams the greatest amount of operational latitude.

This is borne out by the survey results. Figure 6, which summarises survey respondent views on their preferred form of regulation, shows a marked preference for self-regulation where such a preference was expressed.

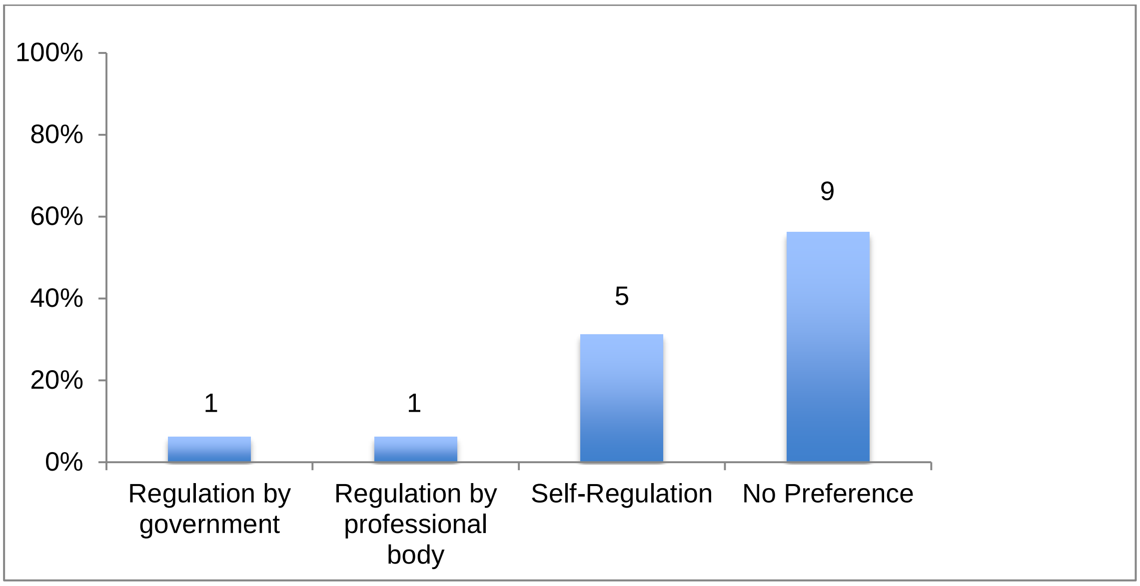

Figure 9: Survey respondents' regulatory preference

20 interviewees (77 per cent), representing all three groups, expressed support for external regulation on two levels. The first of these was the personal level. These interviewees considered that counter fraud staff should

have a professional code of ethics and take personal responsibility for acting in accordance with professional, educational and technical standards.

The second was the organisational level. The same interviewees felt that there needs to be some oversight as to how organisations exercise their counter fraud responsibilities corporately. One interviewee noted that the *CIPFA Voluntary Code of Conduct* for counter fraud operations, published in May 2014, is an attempt to meet this need (CIPFA, 2014).

Those interviewees who expressed an opinion felt that any external regulation should include one or more of the functions listed in Figure 7. From the roles listed in this figure, it can be inferred that there was some support from interviewees for the greater involvement of professional institutes in counter fraud regulation. The prevention of abuse by counter fraud staff is of particular interest. This is because externally imposed regulation, through the enforcement of professional standards, may help limit public service organisations' risk and exposure to challenge. When asked, more than 90 per cent of respondents to the survey stated that liability for their actions lay with the employing organisation rather than individual members of staff.

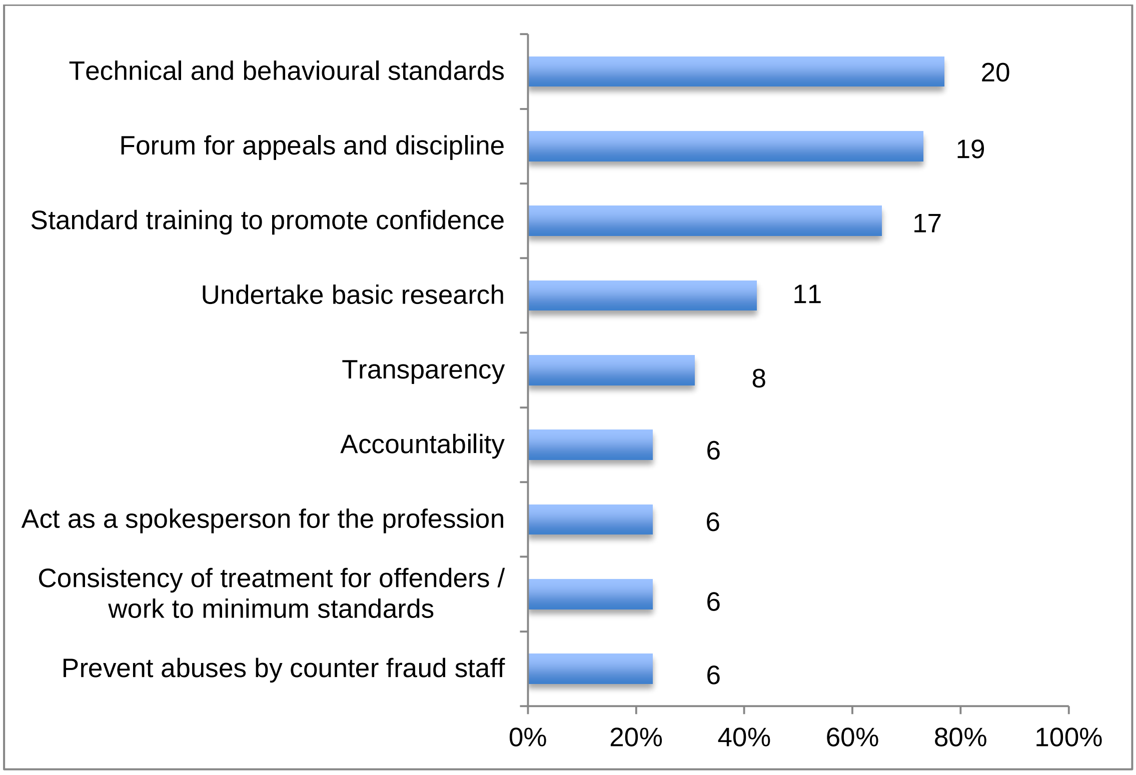

Figure 10: Principal tasks for external regulation

Conclusion

Fraud is a complex crime involving a number of different offences and behaviours. Current actions to deal with it suffer from a variety of hindrances, such as a fragmented legal framework, a lack of core skills, resourcing issues, poor intelligence and data sharing, barriers to collaborative working, a lack of standards and regulation. The UK Government is alive to these difficulties and has published a strategy and set in place a reform programme to deal with them. However, this is at a strategic level only and has yet to tackle some key issues such as how law enforcement can work with civilian counter fraud teams more effectively given that the latter often do not have the legal powers, skills, infrastructure or regulation needed to make this work.

This research suggests that there are inconsistencies within Government policy towards tackling fraud and corruption. The Government's promotion of a zero tolerance culture is difficult to achieve with limited police resources to tackle fraud related issues and the inconsistent legal framework within which civilian counter fraud specialists operate. There is also some evidence that, even if the necessary legal and regulatory frameworks were in place, central government counter fraud teams do not have the basic mix and quantity of skills to make best use of them.

The Government's proposals for managing public sector fraud are thus unlikely to bring about the transformation they envisage. There is insufficient resource within the law enforcement community to tackle the £billions lost to the UK public sector annually from fraud unrelated to the tax and benefits systems; and, the position is unlikely to improve in the short to medium term. Consequently, unless the Government empower their civilian counterparts to provide the complementary service it envisages, the disruption of fraudulent activity is unlikely to occur on the scale required to make significant reductions into losses suffered (Cabinet Office and NFA, 2011b, p. 7; Doig and Levi, 2009, p. 200; Gannon and Doig, 2010, p. 45).

This, in turn, runs the risk of undermining their strategy much of which is centred on fraud prevention. If it becomes clear that the investigative and enforcement capability to counter fraud is sub optimal, and that the chance of avoiding detection and prosecution is high, it is unlikely that those tempted to commit fraud will be deterred, or prevented, from doing so. The Government recognised this by noting that not all frauds are preventable – by even the most robust controls (Cabinet Office and NFA, 2011b, p. 17).

Therefore, the Cabinet Office's response to countering fraud needs to reconcile better the tensions between their desire for an enhanced response to fraud, and the civilian capability to deliver this. There needs to be a recognition that the legal and regulatory environment within which civilian counter fraud services are delivered within Government may be in need of reform. The Government has not indicated that it intends to amend the current legal and regulatory environment – in a way that would support their stated preference for a zero tolerance process. This may explain why more than one half of the respondents appear to accept the current status quo and thus the culture change needed within their organisations, to provide a more effective counter fraud service, is unlikely to occur.

Consequently, the Government's plan to bring about this culture change through improving fraud awareness, through the education of staff and encouraging inter-agency co-operation, needs further development. This much needed culture change needs to filter down to the structures within organisations and the way in which these are managed and controlled. Counter fraud champions and their senior managers should focus more on the role of the counter fraud department in the stewardship of assets and their priority for funding and action. In particular, human resources departments need to work with their finance, internal audit and counter fraud colleagues to undertake a pay, grading and skills audit, produce a training plan and equip the teams properly.

References

Andrews, R., Boyne, G., Law, J., & Walker, R. (2008). Organisational Strategy, External Regulation and Public Service Performance. *Public Administration, 86*(1), 2185-203. doi: 10.1111/j.1467-9299.2007.00695.x

Attorney General's Office. (2006). *Fraud Review Final Report*. London: Attorney General's Office.

Australian Government. (2007). *Best Practice Regulation Handbook*. Canberra. Retrieved from http://regulationbodyofknowledge.org/wp-content/uploads/2013/03/AustralianGovernment_Best_Practice_Regulation.pdf

Baker, S. (2011). *Redacted*. Retrieved from http://www.theyworkforyou.com/debates/?id=2011-03-21b.825.0

Button, M. (2011). Fraud investigation and the 'flawed architecture' of counter fraud entities in the United Kingdom. *International Journal of Law, Crime and Justice, 39*(4), 249-265.

Button, M., Johnston, L., & Frimpong, K. (2008). The Fraud Review and the Policing of Fraud: Laying the Foundations for a Centralised Fraud Police or Counter Fraud Executive. *Policing*, *2*(2), 241-250.

Cabinet Office & National Fraud Authority. (2011a). *Eliminating Public Sector Fraud*. London. Cabinet Office.

Cabinet Office & National Fraud Authority. (2011b). *Fighting Fraud Together*. London: National Fraud Authority.

Cabinet Office. (2012). *Tackling Fraud and Error in Government*. London: Cabinet Office.

Centre on Regulation and Competition. (2004). Why Regulatory Governance Matters. In *Centre on Regulation and Competition* (Ed.), (Vol. 2/2004, pp. 1-4). Manchester: Centre on Regulation and Competition.

Chartered Institute of Public Finance and Accountancy. (2014). *Code of practice on managing the risk of fraud and corruption*. London: Chartered Institute of Public Finance and Accountancy.

Department for Constitutional Affairs. (2003). *Public Sector Data Sharing: Guidance on the Law:* London: Department for Constitutional Affairs. Retrieved from http://www.mentalhealthlaw.co.uk/images/Data_sharing_legal_guidance.pdf

Doig, A., & Levi, M. (2009). Inter-agency work and the UK public sector investigation of fraud, 1996-2006: joined up rhetoric and disjointed reality. *Policing and Society, 19*(3), 199-215.

Fisher, J. (2010). *Fighting Fraud and Financial Crime*. (Policy Exchange). Retreived from http://policyexchange.org.uk/publications/category/item/fighting-fraud-and-financial-crime

Frimpong, K., & Baker, P. (2007). Fighting Public Sector Fraud: The Growth of Professionalism in Counter Fraud Investigators. *Crime Prevention and Community Safety, 9*(2), 130-137.

Gannon, R., & Doig, A. (2010). Ducking the answer? Fraud strategies and police resources. *Policing and Society, 20*(1), 39-60.

Gunningham, N., & Sinclair, D. (2009). Organizational Trust and the Limits of Management-Based Regulation. *Law and Society Review, 43*(4), 865-900.

HM Treasury. (2003). *Managing the Risk of Fraud: A Guide for Managers*. London: HM Treasury.

HM Treasury. (2007). *Government Internal Audit Competency Framework*. London: HM Treasury.

HM Treasury. (2011). *Government Internal Audit Standards*. London: HM Treasury.

Home Office. (2004). *Circular 47/2004: Priorities for the Investigation of Fraud Cases*. London: Home Office.

Hurrell A. (2014, July 27). 'Five years of hell - now I want police and Crown Prosecution Service to apologise' says wrongly-accused former Norfolk psychiatric hospital chief. *Eastern Daily Press*. Retrieved from http://www.edp24.co.uk/news/crime/five_years_of_hell_now_i_want_police_and_crown_prosecution_service_to_apologise_says_wrongly_accused_former_norfolk_psychiatric_hospital_chief_1_3701608

Independent Police Complaints Commission. (2011). *About the IPCC*. Retrieved from https://www.ipcc.gov.uk/page/about-us

Kelly, J. (2015). Crime figures: 'Five million' fraud cases in past year. Retrieved from: http://www.bbc.co.uk/news/uk-34538183

Krambia-Kapardis, M. (2002). A fraud detection model: A must for Auditors. *Journal of Financial Regulation and Compliance, 10*(3), 266-278.

Levi, M., Burrows, J., Fleming, M., & Hopkins, M. (2007). *The Nature, Extent and Economic Impact of Fraud in the UK*. London: Association of Chief Police Officers.

Middleton, D. (2005). The Legal and Regulatory Response to Solicitors Involved in Serious Fraud: Is Regulatory Action More Effective than Criminal Prosecution? *British Journal of Criminology, 45*(6), 810-836. doi: 10.1093/bjc/azi014

National Audit Office. (2012). *The effectiveness of internal audit in central government*. London: The Stationery Office.

National Fraud Authority. (2012). *Annual Fraud Indicator*. London: National Fraud Authority.

National Fraud Authority. (2013). *Annual Fraud Indicator*. London: National Fraud Authority.

Phillips, S. (2012). Non-Law Enforcement Approaches to the Investigation of Fraud. In A. Doig (Ed.), *Fraud The Counter Fraud Practitioner's Handbook* (pp. 75-83). Farnham: Gower Publishing Limited.

Porket, J. (2003). The Pros and Cons of Government Regulation. *Institute of Economic. Affairs, 23*(4), 48-54.

Robson, C. (2002). *Real World Research* (2nd ed.). Oxford: Blackwells.

Samarajiva, R. (2001). Regulating in an imperfect world: building independence through legitimacy. *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media 3*(5), 363-368.

Security Industry Authority. (2014). *Regulation of Private Investigators*. Retrieved from http://www.sia.homeoffice.gov.uk/Pages/licensing-private-investigations.aspx

Snyder, B. (2014). Ernst and Young settles SEC accusations for £4 million. *Fortune*. Retrieved from http://fortune.com/2014/07/14/ernst-young-settles-sec-accuasations-for-4-million/

Wells, J. (2011). *Corporate Fraud Handbook - Prevention and Detection* (3rd ed.). New Jersey: Wiley.

Wiig, S., & Tharaldsen, J. (2012). In regulation we trust. *Work: A Journal Of Prevention, Assessment, And Rehabilitation 41*(2012), 3043-3050.