1 Responsibility

Fraud Awareness Quiz – Question 1

Who is responsible for preventing and detecting fraud in your organisation?

What a mess – how could all this have been allowed to happen?

I am sitting in the boardroom of our new offices in Covent Garden, London. It is March 1991. I am about to present the monthly update report on the progress of the Polly Peck case to Christopher Morris, Fergus Falk and the various other partners and lawyers who together comprise the senior members of the Touche Ross investigation team. It is almost six months since Christopher was first appointed as joint administrator of Polly Peck, charged specifically with investigating the circumstances of the collapse of the company and the activities of its then Chairman and Chief Executive, Asil Nadir. Much has happened since then.

The investigation team has been working hard and the partners are not yet aware of all of the results. I know that what I have to say in this meeting will have a big impact. There are three parts to my report.

I begin by giving an update on the new offices, reminding everyone about the background. We moved in earlier in the month on the advice of our security consultants. These men work for a specialist firm and come highly recommended by the police. They are mainly from an army background in military security and defence intelligence and, having left the army, they are now the acknowledged experts in the UK in all aspects of corporate security and counter-surveillance. Their first piece of advice is to tell us that we need our own premises, separate from Touche Ross's existing buildings. Their reasoning is simple, if extreme: the locations of the firm's main offices in various buildings around London are all well-known; they present an obvious target which, for example, could be fire-bombed by the other side in order to destroy evidence; and the team needed its own secure, self-contained and secret premises from which to run the investigation most effectively. Obviously, as we are now working in the new offices, we took their advice. Somebody in the meeting asks how we came to choose this particular suite of offices. I say that the security advisers located it for us by means of a fairly basic but effective vetting process. They obtained a list of premises with available office space to rent in central London and then proceeded to visit each office. Their technique was very simple. They arrived unannounced at each office in turn, always dressed smartly in business suits and carrying clip-boards. They proceeded to walk through the buildings until challenged. They were looking for the building where the challenge process was both quick and robust. The Covent Garden offices passed these tests (the other buildings visited did not) and they advised us to take them. I then mention the second, more prosaic advantage of being here, which is that these premises have a lot of storage space and we are certainly going to need it, given all the evidence that we are rapidly accumulating on the case. The offices are now the base for the entire investigation team. Everyone agrees with me that they are ideal for our purposes. I say one more thing about the new premises: everyone can speak openly and freely in today's meeting because the security consultants came in earlier this morning and carried out a "sweep" of the boardroom to make sure that it is free of any surveillance bugs or listening devices. There are a number of nervous smiles around the room at this news.

I now turn to the more serious matter of what looks like some major control weaknesses at Polly Peck. The team has made progress with one of the key areas of the investigation – asset tracing. We have already come across an array of money transfers out of the London head office bank account. As a court-appointed administrator, Mr Morris has the power to compel each of Polly Peck's various bankers to supply details and paperwork of all transactions going across the account. All the requests for this information have now been sent out and the replies from the banks are starting to come in. Our analysis and review work is at an early stage but there is one feature that is starting to cause us some concern. We can identify a series of large cash payments going out of the account, all for round-sum amounts (e.g. £100,000 or £150,000 or £250,000 etc.). These payments have been posted in Polly Peck's books to the inter-company account with Unipac, the group's main trading subsidiary in the TRNC. However, from the initial review of the information received from the banks, it seems that much of the money does not arrive there! The money appears to be transferred initially to accounts in the Channel Islands, from where it is splintered and diverted to a variety of other destinations, all in accordance with instructions from Polly Peck. We will be able to confirm these destinations when we receive all the documentation from the banks in due course. I mention also that the purpose of these transfers is entirely unclear at present. Why does Unipac, a very profitable company (at least, according to the accounts) apparently need so much cash from London? There is silence in the room now. I come to the most disturbing part. It seems that all of these transfers were approved by Mr Nadir himself and were paid away on his sole signature. Mr Nadir was able to do this because, we believe, he enjoyed sole cheque signing powers, to an unlimited amount, on the Polly Peck bank accounts. If this is indeed the case, then there were no effective controls over his use of corporate funds whatsoever, despite Polly Peck being a listed company.

I can see that this news has certainly got everyone's attention. There is more to come.

My third point is to inform everyone about the contents of a report just in from our undercover investigators in the TRNC. I need to say something about these undercover investigators. Originally, we had assumed that members of the investigation team would soon be travelling to the TRNC to review the Polly Peck group assets there. Questions of the ownership of assets in the TRNC and their recoverability were proving to be far from straightforward. For example, we could see from the accounting documentation that tens of millions of pounds of Polly Peck money were apparently located in the TRNC, held on deposit with three local banks. The joint administrators wrote to these three banks, instructing them to remit this money to London, only to receive replies expressing regret that they were unable to comply with the instructions because the funds were "blocked". This sounded highly suspicious and clearly we needed to resolve the position. However, our security consultants strongly advised against any members of the investigation team travelling to the TRNC. In their view, the threat of violence can never be ruled out when the stakes are as high as in this case. Also, the UK has no extradition treaty with the TRNC and they felt it was highly likely that if any of the team went out there the individuals would not be allowed to leave. Given the influence of Mr Nadir on the island, they felt that any Touche Ross representatives working in the TRNC would be detained at the end of their visit to be used as bargaining chips in subsequent negotiations. So, rather than travel ourselves we decided to hire two investigators to take a look at the situation on the ground in the TRNC, in a covert capacity. Accordingly, the investigators had travelled secretly to the TRNC three weeks ago and we received their first report only the day before.

So, I take the meeting through the key points in the investigators' report. I know that they will be as shocked at its contents as all of us who read it yesterday were. I say that the investigators have visited the three banks in the TRNC that claim to be holding Polly Peck's money. Photographs of the banks are attached to the report and I hand these out around the table. The banks look small, shabby

and run down even, not places that give confidence that they should be holding millions of pounds of Polly Peck's funds. I now come to the most alarming part of the report. The investigators have also been able to check the ownership structure of the banks. It turns out that all three of them are owned by Mr Nadir himself! Everyone in the room is now looking around at each other.

These are all senior accountants and lawyers, with years of experience of looking into corporate collapses and scandals. So, a number of them no doubt suspected that something like this had been going on. However, the reality still comes as a big shock to most people in the room. There had been no disclosure of this obvious conflict of interest with the banks in Polly Peck's annual Report and Accounts and of course the lack of an effective control over Mr Nadir's cheque-signing powers had not been disclosed anywhere. Fergus Falk says something quietly, almost to himself, but it captures exactly what we are all feeling: "Well, well, well, what a mess – how could all this have been allowed to happen?"

Introduction

Fraud is a significant risk to the profits and reputation of all businesses today. The starting point for any organisation in fighting fraud effectively is a clear understanding of where responsibility for managing this risk lies. Fergus Falk's comment, back in 1991, was absolutely the key question – exactly who was responsible for the problems that we were uncovering at Polly Peck? This Chapter provides directors and managers with an overview, a framework within which effective governance, risk management and internal controls can be developed. There was no such strong framework in place at Polly Peck and it was this structural weakness that made it so vulnerable to fraud.

This Chapter starts with a look at how the delegates on my courses and workshops over the years have answered the responsibility question in the Quiz. The answers enable us to draw a number of conclusions on areas where businesses can improve their approach. Next, we look at the powerful Responsibility Framework and consider the governance, risk and controls theory that underpins it. There is then a section introducing the topic of the responsibility of auditors (both internal and external) in preventing and detecting fraud. This is an important area because audit responsibility is often misunderstood and also, in practice, many organisations place too much reliance on traditional audit techniques to fight fraud. Finally, the Chapter closes with an overview of the modern approach to managing fraud: it is a strategic, risk-based approach that is rooted in governance mechanisms, with resources devoted to "upstream activities" of prevention and deterrence, backed up by modern detective techniques and access to specialist investigation resources.

This Chapter emphasises from the outset the importance of factors such as corporate culture, tone at the top and awareness of risk in the successful management of fraud threats.

As an example of best practice in strategic fraud risk management, consider the following comments in an extract from my interview with Frazer. Frazer is a senior manager in a large government department in the UK's public sector. I began the interview by asking him what level of priority was given to fraud in his organisation. This is his reply:

> Fraud risk management has been reported by the Chair of the Audit and Risk Committee as one of the top three priorities for our board, so it's given very high priority. It's primarily driven by guidance on how we manage public finances and we are required to have in place a process for understanding and managing cases of fraud so it's managing public money. Our Accounting Officer is accountable to make sure we have that and it is treated extremely seriously by our most senior officers.

There is a very powerful message here. Directors and managers need to understand that, although anti-fraud controls are crucial (and these are discussed at length throughout the book) the culture, tone and risk profile of their business will provide the entire context in which these controls are set.

Another important point (and one of my key messages) is that if fraud is to be managed successfully, it must not be looked at in isolation but rather it should be put in its proper context of business risk. All organisations need a proper understanding and assessment of fraud risk within their own business profiles in order to be able to design effective and proportionate controls to manage the various threats that fraud poses both to their profits and to their reputation. This is the essence of taking a risk-based approach.

Before we go on to discuss the risk-based approach, we begin with the Quiz and the answers to Question 1.

Answers to the Quiz

Fraud Awareness Quiz – Question 1

Who is responsible for preventing and detecting fraud in your organisation?

The first question of the Quiz addresses the issue of responsibility directly. The answers given by delegates on my courses and the points arising in the subsequent discussions provide me with a good indicator of how effective fraud prevention, deterrence and detection is likely to be within the individual organisations represented in the room on a particular day. When taken together over the years, these answers provide a useful insight into a number of general attitudes to fraud that are common in business organisations today that can lead to vulnerabilities in day-to-day practice.

The answers given to the question will vary of course depending on the mix of experience and backgrounds of delegates on any one day. Nevertheless, there are similarities and patterns from which conclusions may be drawn. Set out below are the most often repeated comments and discussion points that I have heard, in order of frequency:

- **"Everyone".** Most delegates write down one word as their answer to this question – everyone. This is now by far the most popular response I get in any discussions around responsibility, not only when discussing fraud specifically but also in a wider risk management context too. It was not always so: 12 years ago when I started lecturing on fraud most people would nominate specific individuals or departments such as "Internal Audit" or "Security" or "Compliance" or even the Money Laundering Reporting Officer as having responsibility. Today there is much greater awareness of the power and effectiveness of getting everybody in an organisation involved in the fight against fraud. However, the one-word answer of "everyone" can seem to be a little routine, a little superficial sometimes. It needs to be tested further (see below). In addition, a more forensic approach to the question of where responsibility lies in business is required.

- **"Internal Audit".** Many delegates believe that internal auditors have specific responsibility for preventing and detecting fraud. Interestingly, external audit is almost never put forward as an answer. "Internal audit" is of course most often given as an answer by those delegates who are themselves internal auditors. In the subsequent discussions it is sometimes unclear on what experience their answer is based, because most of these delegates admit that they do not themselves carry out specific anti-fraud auditing. Many have been involved in investigating

frauds that have occurred but this is not the same thing – it is reactive work, responding to a specific situation revealed by a tip-off or otherwise. It is not proactive fraud prevention and detection work. We will look at aspects of fraud investigations in Chapter 9 of the book but it is important at this stage to emphasise that if internal auditors are going to be involved as fraud investigators they need two things to be effective in that role. First, they need some tailored investigation training – on the rules of evidence, on how to handle themselves when conducting interviews under pressure etc. Secondly, they need access to modern auditing tools – in particular computer-assisted audit techniques ("CAATs"). Unfortunately, most of the internal auditors who attend these sessions have neither. The role of auditors (both internal and external) in anti-fraud work is sometimes poorly understood and reliance on a traditional audit approach is often ineffective. This is discussed in detail later in the book.

- **"The board".** Although there is greater awareness today than there was in the 1990s of the responsibilities of the board of directors in preventing and detecting fraud, this answer has often to be teased out of delegates during discussions. This is more than a little surprising. The simple fact is that those individuals at the top of an organisation (whether directors, partners or a senior management team) are ultimately responsible for the risk management systems and internal controls operating in every business. Fraud falls firmly within this framework and yet this basic governance point does not seem to be widely understood.

- **"Management".** It is also surprising that this answer is not given more often. Management, in particular departmental heads and line managers, have prime responsibility for managing risk in business today. However, delegates often have to be prompted and reminded of this. This makes me question whether in practice managers are sufficiently "hands on" in dealing with risk. If not, this is a significant weakness, especially in an area like fraud. For example, it would be very dangerous for any organisation if its Head of Procurement was not well aware of fraud risks in the supply chain and buying processes of the business.

- **"The Risk Manager".** The perception of fraud as a business risk is increasing but unfortunately few delegates seem aware of one of the key principles of modern risk management, namely that "risk devolves to the line". In other words, effective management of risk is carried out by line managers and departmental heads, rather than by nominated individuals. The importance of the role of the Risk Manager has increased following the recent financial crisis, when an under-pricing of risk in financial services in particular was one of the factors in a number of large institutions either failing (e.g. Lehman Brothers) or being compelled to seek government help (e.g. the Royal Bank of Scotland). The role of the Risk Manager is one of engagement and influence, of coordination, of reporting – not of managing risk directly. The day-to-day management of risk has to be devolved to managers throughout the business if it is to be effective.

- **"Security".** A much rarer answer these days, other than by delegates from financial services and insurance institutions or from the public sector, where organisations typically employ teams of investigators and specialists to deal vigorously with the risks posed by organised crime gangs, benefit cheats and other external fraud threats.

There are never any right or wrong answers to questions around responsibility but what I would say is that most of the responses that I am given are incomplete. In fact I would go further and say that it is very rare indeed for a delegate to give me what I would regard as a complete answer to this question. The answer that I always look for, and try to steer the discussion towards, brings together three of the answers given above: first, the board and senior management team; secondly, managers – in particular departmental heads and line managers; and thirdly, everyone.

These elements combine to form the powerful "Responsibility Framework" which we will turn to shortly.

Before discussing the Responsibility Framework, there is one other important point that I want to make arising out of the discussions with delegates on the responsibility question. As mentioned above, by far the most common answer that I am given to this question is "everyone". It is of course encouraging that managers and staff seem very well aware of the importance of this inclusive concept, no doubt from other training they have received in areas like risk management. But perhaps because I hear it so often, I have grown concerned that this has become simply a default answer, a stock response without real meaning or reference to what is actually happening within businesses. To help explore what the answer "everyone" might mean in practice I often ask a supplemental question as follows:

> If I were to go to your offices, pick three people at random from your organisation (they could be the Chairman, the receptionist, middle managers, clerks - anyone) and ask them the question "who is responsible for preventing and detecting fraud in your organisation", are you confident that I would receive the same answer that you have just given me, namely "everyone"?

Amazingly, I have worked with very few delegates who have given a confident, unqualified "yes" to this supplemental question! It does happen, but it is rare. The implication of this is that the answer "everyone" is indeed a default option, an idealised response or a "best practice" solution. It is likely that many organisations are failing in practice to get all of their staff involved in the fight against fraud. Awareness of responsibility is a basic requirement for good risk management.

Consider the following. If a hypothetical fire (of whatever sort) were to go off in your business how would you want your people to react? Pretty obviously, you will want the first person who becomes aware of it to be the one who shouts "Fire!" You absolutely do not want that employee to leave it to someone else because the individual does not consider it to be his or her responsibility. This principle applies to fraud as it does to any other area of risk.

Poor awareness of responsibility is a serious weakness in any organisation. The answers to the first question of the Quiz that I have received over many years lead me to believe that, in the specific area of fraud risk management, it is a serious weakness that is widespread in business today. It needs to be addressed proactively through training and the quality of supervision by line managers, which in turn requires the commitment of time, resources and money by the board of directors. This brings us back to the Responsibility Framework.

Responsibility Framework

Introduction

The starting point of effective risk management (and fraud is of course a risk) for any organisation is to have a clear awareness throughout the organisation of responsibility at three levels: the board of directors and senior managers; line managers and departmental heads; and every individual member of staff. An overview of responsibility at each of the three levels is as follows:

- **The board and the senior management team.** The people at the top establish the values of an organisation and set policy. The collective body (we are calling it here for simplicity "the board")

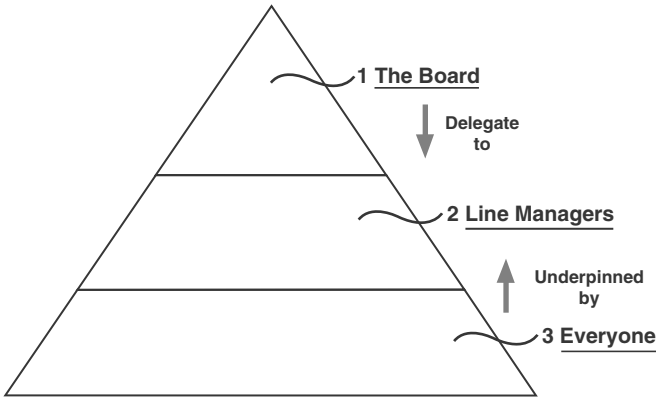

Diagram 1.1 Responsibility Framework

has ultimate responsibility for managing risk and for putting in place an appropriate system of internal controls to achieve this.

- **Line managers.** The board delegates to line managers. It is the role of managers to implement board policies on risk and control. So, managers should identify and evaluate the risks faced and design, operate and monitor a suitable system of internal control which implements the policies of the board.

- **Everyone.** All employees have some responsibility for risk management and internal control as part of their accountability for achieving their objectives. The participation of everyone underpins the framework.

I have coined the term "Responsibility Framework" for these roles and responsibilities. The framework can be represented diagrammatically as a triangle as shown in Diagram 1.1 above.

I always emphasise the importance of the Responsibility Framework to my delegates – both generally in terms of risk management and internal controls and of course specifically around managing fraud threats. I find the responsibility triangle diagram very useful for these purposes because it provides a simple visual picture of the framework.

International best practice

Both the concept of the Responsibility Framework and its representation as the triangle diagram are rooted in best practice corporate governance and risk and controls theory. I have based them directly on the report "Internal Control: Guidance for Directors on the Combined Code" ("the Turnbull Guidance") which was published in the UK in September 1999 and is at the time of writing being updated. The UK's Turnbull Guidance is one of the key internal control frameworks that have been developed around the world in recent years.

We need to look also at the US for ideas on responsibility within organisations. It has been the Americans who have led the way on this with two key control frameworks being developed in the US in the last 20 years. First, the "Internal Control – Integrated Framework" developed in 1992 by the Committee of Sponsoring Organisations of the Treadway Commission ("COSO"). This is currently being updated but it is still regarded as setting the standard for internal control frameworks around the world. The second key development affects those corporations with a

listing in the US who need robust control frameworks in order to comply with the requirements of the Sarbanes-Oxley Act 2002 ("SOX").

All of these three frameworks are different but mutually compatible and each will be reviewed in some detail in Chapters 5 and 6 of the book.

Practical application

It is important to say, however, that whilst the Responsibility Framework is based upon international best practice, it is not simply a theoretical construction. It is to be found operating in practice day to day in those businesses with a strong controls and risk management culture all over the world.

As an example of this, the importance of the Responsibility Framework is understood absolutely by Sharon, the deputy CEO of a large financial institution in the Caribbean. Consider the following extract from my interview with her carried out for the purposes of this book. I started the interview by asking her the same question about the responsibility for preventing and detecting fraud that we have looked at as Question 1 in the Quiz. Here is Sharon's reply:

> Steve, you would have to start off with something that is just so complicated! Well, I should say first the responsibility for ensuring that fraud is dealt with in a certain manner is vested in the executive and in the board. That's the way because obviously the leadership has to set the tone within the organisation and that is one of the things that is clear in our organisation. But then we say to our staff that everybody in the organisation is responsible for detecting fraud. You need this because it is only through your people in your branches saying if they see somebody doing this or doing that you are going to find out about fraud. You are not going to know sitting in a head office what somebody might be doing in a branch at the other end of the island! So therefore what does that mean for us? Firstly we have to develop the policies. We have determined in our organisation that there is to be zero tolerance for fraud. What that means is that it does not matter whether the fraudulent act results in the end in an actual loss to the organisation because the person carrying out the act simply does not remain with us any longer. And it does not matter how long they were with us – they have to go. That is easier said than done. It is difficult to do but once you say it then you have to live by it and people have to understand it that way, which is why it is so important to have buy-in at the more senior level and line-management level with respect to this.
>
> And people in the organisation understand that now. So even when they think that somebody finds somebody who has done something fraudulently and they know it is fraudulent and even when they know the bank hasn't lost any money as a result, they also know the person can't remain in the organisation and we have set that awareness for ourselves. Another major thing for us is that we have to constantly train our people. You have to train people, let people understand what a fraudulent act is and then understand why it is important for us that we have zero tolerance. They need to understand what is so wrong about this, what did they do, how fraud at the end of the day can destroy an institution and if it destroys the institution then you yourself will not have a job and we need to keep connecting those dots all the time. So the thing we do, after we have the policies, is we do the training and it is very important in the training to keep showing the live example of what has happened, scenario-based training as you would call it.

> And then of course what we do is we say to the managers of the branches and the business units that the cost of the fraud is to hit your bottom line, it does not come into head office. So you are very careful, you want to make sure managers understand their responsibility because they have to manage this, especially now with the way the market is. When there is pressure to make results you can't have all this fraud affecting your P & L. If there is fraud in one of our branches it's actually the branch itself that bears the cost, it's making clear to the branch manager that he's the point man on this, he's the guy who has to manage this. Those are the things that people need to learn and understand.

Sharon clearly "gets it" and so does her bank. She sets out here a very practical approach to fraud risk management and mentions two of the key ingredients that we will look at in detail later: the importance of culture (in the case of her bank it has a "zero tolerance" attitude to fraud) and the importance of getting the message conveyed to staff through training with senior staff members taking the lead.

The linkage between risk management and internal controls

Overview

We will look at both risk management and internal controls in detail in later Chapters of the book. It is useful at the outset, however, to set out some fundamental points regarding risk and controls and how the two inter-relate. Directors and managers need a good understanding of how this relationship works if their organisations are going to be able to manage fraud risk effectively. My discussions with delegates on the courses suggest that there may be some confusion as to how risk and controls actually relate to each other in practice, particularly for those who are not from a financial or an accounting background.

So, here are five key ideas that directors and managers should always bear in mind when looking at risk and controls:

- **Risk, broadly defined, means uncertainty.** In a business context risk equates to "uncertainty of outcome". If a company knew for certain what was going to happen in the future there would be no risk, but of course this is not possible. Consequently, risk must be managed.

- **Risk should be optimised, rather than minimised.** That is to say, every business should be looking to optimise the amount of risk it is prepared to accept in the pursuit of value, with the crucial reference point always being the risk appetite of each individual business. We consider the concept of risk appetite further in Chapter 4. Businesses will never be able to grow or achieve their corporate objectives simply by minimising risk. This is an important point and one that is not always readily apparent. As an example, I am often asked to speak about risk management at conferences and I sometimes find it an interesting exercise to ask delegates to raise their hands if they agree with the following statement: "We are looking to minimise risk in our business". There are always more hands raised than are not raised in answer.

- **Risk is dynamic, it changes all the time.** Internal controls are not dynamic, however. In many organisations, especially mature businesses, control systems and procedures have evolved slowly over time and may be characterised as being essentially historic, as remaining "anchored in the past". As a result, gaps often appear between risks (which are changing) and controls (which are slow to react to those changes). There is real danger for all businesses if these gaps are allowed to grow too wide.

- **Risk determines controls, not the other way around.** Internal controls exist for many reasons but fundamentally they are there to help to manage risk. It is simply not possible, therefore, for any organisation to have an effective and efficient system of internal controls in place unless it is based on a thorough, systematic and ongoing assessment of risk in the business.

- **Understand the essence of the control concept.** Key aspects of controls need to be understood also, in addition to the ideas on risk. Here, there are two crucial questions about control effectiveness. All directors and managers need to know what these questions are, they need to ask them regularly within their businesses and they need to understand the answers before they can properly conclude on the adequacy of their internal control systems. The first key question is: "are the controls effectively designed?" The key reference point here is risk and the basic equation is: the higher the risk, the stronger the controls. For a control to be properly designated as "strong" generally it will require the involvement of a senior manager or an experienced member of staff. As a matter of principle, high-risk areas should not be allocated to junior or inexperienced members of staff. The second key question is: "are the controls working effectively, in accordance with the control design?" Just because a control or procedure happens to be written down in a manual does not mean that it will be carried out in practice. From my experience, internal auditors often spend more time on the second question than on the first. They look in particular for evidence that controls are working rather than first considering whether the design of the control is appropriate. This is a mistake.

Control design linked to risk

Before moving on to look at the importance of evidence and the evidence-based approach, there is one point coming out of the above analysis that is worth emphasising. Controls need to be properly designed if they are to be effective. Good control design is impossible without good risk analysis. This is as true for fraud as it is for any other area of risk in business. One of the fundamental requirements for effective management of fraud is for an organisation to understand where the threats are in its own particular business model. This requires a thorough, systematic and informed assessment of fraud risk in the business. We will refer to this later as a "fraud risk profile". The great majority of delegates that I work with tell me that their own organisations do not have such a fraud risk profile. In reply I tell them that this is a serious weakness, so that this is often the first key action point for delegates arising on the day.

The importance of evidence

Introduction

Evidence is critical in discharging management responsibilities in business today. One of the big changes between how business was conducted in the 1990s and how it is conducted today as we move into the second decade of the new millennium is the emphasis now put on decisions and actions to be "evidence-based". In the previous century this was not so. Then, executives and managers would routinely act on decisions based on judgement calls arising out of discussions that were not written down or on information not retained or simply on "gut feel" – a phrase that, in the business context, usually refers to pattern-recognition, the instincts that make a manager good at his or her job. It would be both risky and unprofessional to take this approach today. Courts of law, regulators, auditors and other interested third parties look for evidence to support the decisions taken, especially where those decisions turn out, with hindsight, to have been sub-optimal – an executive euphemism for what are commonly known as mistakes! If there is no evidence to support the decision-making process and it turns out that mistakes have been made, then the directors and managers concerned are always vulnerable to

accusations that they had not discharged their responsibilities properly and had therefore been negligent.

Examples

There are many examples today of the need for business decisions to be based firmly on evidence. Consider the following three examples that I use regularly in my training courses:

Example: external audit questioning. The first is from my own experience as an external auditor. I started work in 1979 as a trainee accountant in London. From time to time I would be required to ask questions of the Finance Director of the audit client that I was working on. Here my duties were very clear: I was to be fully briefed and prepared, arrange for a convenient time to meet the Finance Director, go in armed with my notebook and questions, ask the relevant questions, record faithfully the answers given and . . . nothing else. That was it! If the answers to any of the questions I raised were considered to be of fundamental importance to the audit opinion, the audit partner would include the question concerned in the firm's "Letter of Representation" addressed to the board of directors of the client company, who would be required to sign it before the audit opinion was signed off in order to provide formal written confirmation of key representations made to us during the course of the audit. If I was starting my audit career again today I would do everything as before (obviously my notebook would now be replaced by my netbook!) but with one crucial addition. On completion of my meeting with the Finance Director I would have to carry out work myself in order to obtain sufficient, reliable, independent corroborative evidence that what he or she told me was actually true. The whole catalogue of corporate scandals involving people at the top of major corporations in the intervening 30 years (BCCI, Barings, Maxwell, Enron, WorldCom, Refco, Parmalat, Société Générale, Madoff and of course Polly Peck amongst many others) has destroyed forever the myth of self-evident senior management probity, honesty and integrity.

Example: anti-money laundering. My second example relates to the fight against financial crime in its broadest sense – that of anti-money laundering and counter-terrorist financing. The 21st century has seen a marked increase in the rigour with which the authorities around the world have attempted to combat money laundering and the financing of terror. The terrorist atrocities in the US on 11 September 2001 increased the momentum here because of the realisation that much of the money needed by Mohammed Attah and his co-terrorists from al-Qaeda to prepare for the attacks (to pay for food, accommodation, training courses to learn how to fly aeroplanes etc.) was sent to bank accounts they had set up in the US from banks in Germany and the Middle East using standard bank transfer mechanisms. One consequence is that terrorist financing since that time has been closely coupled with money laundering in terms of the law and regulations. Financial institutions are now required to have measures in place to prevent and deter money laundering and terrorist financing and to report any "suspicious transactions" promptly to the authorities. Legislation such as the USA PATRIOT Act 2001 and the Proceeds of Crime Act 2002 in the UK place significant personal responsibility on nominated officers (usually the Money Laundering Reporting Officers or "MLROs") in this regard. Potentially, these individuals could end up in jail if they are found to have been negligent in carrying out their duties. It is therefore imperative that MLROs document fully the reasons for all decisions taken. This applies in particular in situations where the MLRO has taken the decision that a transaction reported to him or her by a member of staff as being "suspicious" is not to be reported onto the authorities because their own investigation has shown it not in fact to be part of a money laundering or terrorist financing scheme. If subsequently this decision turns out to have been wrong, so that a money-launderer and/or a

terrorist has indeed been allowed to take advantage of the system as a result, it is critical that the MLRO is able to point to the evidence of his or her notes showing that, in all the circumstances available at the time, the decision taken was reasonable. Without the evidence the court is likely to conclude that no work was carried out, with the result that the MLRO could well end up in jail for negligence.

Example: UK Bribery Act 2010. Another example can be found in the UK's Bribery Act 2010. We will look at the Act in detail later in the book – it is highly relevant because, in my view, bribery and corruption should properly be viewed as important component parts of corporate fraud, as will be demonstrated in the next Chapter. The key point to make on the Bribery Act at this stage is that the only defence to the new and far-reaching section 7 offence under the Act of the failure of a commercial organisation to prevent bribery is that, despite a particular case of bribery, the organisation in fact did have "adequate procedures" in place to prevent and deter bribery. Examples of what these procedures might be are provided in guidance issued by the Ministry of Justice and include such measures as a bribery risk assessment, a zero tolerance anti-bribery policy signed off by the board, appropriate policies on gifts and hospitality, and robust controls such as whistleblowing hotlines and staff training programmes. The essential feature though is that all of these measures and procedures must actually exist. For example, there must be evidence of the training being carried out, with a register showing the dates when the training took place and the names of those who attended.

Evidence of management of fraud risks

This focus on evidence has as much importance for fraud as it has for all other areas of risk management. As we have seen, it is necessary that awareness of responsibility for preventing and detecting fraud exists at all levels if an organisation is to have a solid foundation for the management of fraud risk. Equally important, however, is that the organisation is able to point to policies, procedures, controls and behaviours that demonstrate that the Responsibility Framework is real and that it exists in practice and not just in theory. Governance and anti-fraud controls are discussed in detail throughout the book but as examples of minimum standards here the following should apply:

- An anti-fraud policy statement. There should be a clear statement by the board, signed off by the Chairman or CEO, of the organisation's robust attitude towards fraud and the severe consequences for anyone attempting fraud against the organisation.

- Line managers should have their responsibility for managing risk in their departments set out clearly in their annual objectives. With this having been set, the appraisal process should pick up actual performance in this area. This provides managers with a clear incentive to perform in this area.

- All managers and staff should receive appropriate anti-fraud awareness training, both on induction and also re-enforced periodically thereafter. Without this it will be difficult indeed to be confident that everyone in an organisation is aware of his or her responsibilities in fraud prevention and detection.

If measures such as these ones (and others) are not in place, the board and senior management will have great difficulty in demonstrating that they have discharged their responsibilities to minimise fraud threats adequately. In the absence of any anti-fraud policy statement from the board, without risk management featuring in managers' targets and appraisals so that managers have an incentive

to perform in this area, and with no anti-fraud training programmes in place it will be difficult indeed for any organisation to claim with credibility that it has taken all appropriate steps to manage its fraud risk effectively.

The role of audit in fraud prevention and detection

Overview

Audit is often thought to play a crucial role in reducing fraud risk. Indeed, if members of the public were to be canvassed at random and asked whether auditors were responsible for preventing and detecting fraud, I have no doubt that the answer would be a resounding "yes"! Much of this conviction might be to do with popular misconceptions about what auditors are actually there to do – there is little clear understanding of the roles of either internal auditors or external auditors outside of the respective auditing professions. However, in my experience, directors and managers also place too much reliance on traditional auditing to provide protection against fraud. Traditional auditing, as we shall see later in Chapter 6, will include a review of systems and controls in conjunction with a more detailed look at the documentary evidence for "samples" – a relatively small number of transactions, selected at random. The sample sizes will either be based on the laws of probability or on judgement. None of this should provide assurance to senior management that any frauds that are being committed in their organisation will be detected by the auditors.

Little training for auditors on fraud awareness

A big part of the problem is that auditors receive very little fraud awareness or investigation training. This was made absolutely clear to me by Teresa, an experienced internal auditor who has headed up internal audit departments in the past and is now a member of the audit committee of a local authority in the UK. This is what she told me during our interview about her own experiences of fraud and her training:

> I think in general, during my time as an internal auditor there was probably very little time spent on formal fraud training. Probably the only time I came across fraud was in one of the organisations I worked for and then purely by chance. I just happened to stumble across something which was relating to the very old fashioned pension incentive scheme payments, basically payments to move people out of housing into private, rented homes. You had to fulfil certain criteria and there were many letters on file and I have to admit, when I read them, I thought it can't possibly be a fraud because it's too well documented to be a fraud – but of course it was! Again, that was kind of I had to learn on the case if you know what I mean because other than technical training through the ACCA (the Association of Certified Chartered Accountants) I really knew very little about it. So I'd say on a day-to-day basis other than stumbling across something like that I probably would spend very little time on it. Other than maybe, if we were doing our own audit programme looking at the kind of fraud risk element within it, but again you know very little actual time would have been spent on fraud. I think that it probably wasn't until I became the head of an internal audit department when you sort of suddenly realise actually how these aspects link together in terms of internal audit, counter- fraud etc. and how you know one can feed into the other and you can become much more effective. Of course I was working in the local authority at that stage with a trained team of fraud investigators. I undertook my own training then as well so that I could understand what they were talking about and more about the risk of fraud within each organisation.

Teresa points to a lack of understanding and focus on fraud that is prevalent in many of the internal audit departments that I have worked with myself. Training for auditors is crucial, as Teresa's comments indicate.

Problems and remedies

In my view, traditional auditing simply does not "cut it" in terms of effective anti-fraud work. There is often a poor appreciation and awareness of fraud risk amongst an internal audit team. The small sample sizes used make it extremely unlikely that any fraudulent transactions that might be in the system will actually be selected for review during the audit process and often fraud as a business risk is never even discussed during the audit. External auditors are required by their standards to consider the issue of fraud in a financial statement audit but there remains considerable scepticism amongst the delegates on my courses about the effectiveness of external auditors in preventing and detecting fraud.

However, directors and managers need to know that there are a number of ways in which auditors can be highly effective in the fight against fraud. The use of "surprise audits", specific fraud audits carried out using a more informed assessment of risk, together with audit tools that enable data mining to take place, are all examples of how to improve audit effectiveness in this area. We will look at both the limitations of traditional auditing and more modern, alternative and effective audit approaches in more detail later in Chapter 6.

The strategic approach to managing fraud risk

Best practice guidance

In 2008, an important piece of anti-fraud guidance was published entitled "Managing the Business Risk of Fraud: A Practical Guide".[1] This work was sponsored jointly by: The Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners. This guidance makes the key point that "diligent and on-going effort" is needed if an organisation is to protect itself against significant fraud threats. It sets out five key principles for proactive fraud risk management as follows:

- **Principle 1**: a fraud risk management programme should be in place, as part of the organisation's governance structure. This will include a written policy stating the expectations of the board of directors and senior management regarding managing fraud risk.

- **Principle 2**: there should be an assessment of fraud risk carried out by the organisation periodically to identify specific threats and changes to the risk profile that need to be controlled and mitigated.

- **Principle 3**: the organisation should have prevention controls and techniques in place to avoid potential key fraud risk events.

- **Principle 4**: the organisation should have detective controls and techniques available to uncover fraud events when preventative measures fail or unmitigated risks are realised.

- **Principle 5**: a reporting process should be in place, together with a coordinated approach to investigation and corrective action. This should help ensure that potential fraud is dealt with in an appropriate and timely manner.

This is powerful and best practice guidance. In my view it is essential that all organisations adopt this strategic approach in practice if the fraud threat is to be managed effectively. In fact, I have been emphasising these principles to my delegates for years in a slightly different format, one that I have termed the Fraud Risk Management Framework.

The Fraud Risk Management Framework

Introduction

This framework is a very simple and powerful way of demonstrating the key components of fraud risk management architecture. It is neatly summarised in Diagram 1.2. I like to take my delegates through the framework in the following way, always starting by pointing to the box at the bottom of the diagram headed "Investigation" and telling them a little of my early experiences as an international fraud investigator. There are five stages in my description to the delegates, as follows:

1. Overview of the framework

I first started working in the forensic and fraud auditing area in the early 1990s. At that time very few businesses in the UK had anything approximating to a fraud risk management programme. Most directors and managers that I spoke to at the time refused to admit that fraud was a problem at all, with a typical attitude being: there has never been any fraud in our business, our people are honest and we trust them. It was very frustrating at times. I remember when I was in forensics at Touche Ross trying to pitch an anti-fraud risk profiling product that we were working on to the Finance Director of a travel company and being told: "that's quite interesting, but what has it to do with us? We do not have any fraud in our business." Just as he was saying this, his secretary came in with a number of cheques for him to sign, which he duly did without even stopping to look at them. I remember thinking at the time that it was perhaps no coincidence that this business had never discovered any fraud!

2. Investigation

During the 1990s the attitude of business to fraud was fundamentally reactive. Essentially, directors and managers would hide behind the fiction that fraud "never happens here" and

Diagram 1.2 Fraud Risk Management Framework

keep their fingers crossed. Typically, on discovery of any form of financial crime, there would be an internal investigation but very rarely would this be reported to the police. So far as managing risk went, they would rely on some form of fidelity insurance cover if the crime was significant and look to that to reduce the financial impact of the fraud.

This reactive approach is still adopted by many businesses today but it is becoming less common. Now, directors and managers are looking more to investing resources in the so-called "upstream activities" of fraud prevention and deterrence. There are various reasons for this, most notably a greater realisation of the importance of reputation in business and the need always to protect the brand. Nothing torpedoes reputation more quickly than a fraud scandal. The other main reason is more pragmatic. The insurance industry is now much less inclined to pay out on a fraud claim without carrying out some review work first. Insurers expect their clients to have in place adequate measures to prevent fraud and, if this is not in fact the case, will seek to avoid paying out under the policy on the grounds that their client has been negligent in failing to put proper systems and controls in place and has therefore contributed to the fraud.

Of course it remains the case that fraud events need to be investigated thoroughly and professionally. All organisations need to have access to investigative expertise, either internally or by using an external source such as forensic accountants or the police. We will look at fraud investigations in detail in Chapter 9 of the book.

3. Prevention and deterrence

The modern approach to fraud focuses first of all on prevention – the policies, controls, training and communication that organisations use to try to stop fraud from occurring. There are a variety of anti-fraud prevention controls available, from generic controls like segregation of duties and delegation of authority through to specific measures such as mandatory vacations and fraud awareness training. Some are more effective than others, and all must be seen in the context of the particular circumstances and characteristics of each individual organisation. We will discuss anti-fraud prevention controls in detail in Chapter 7 of the book.

The bridge between the first box ("Prevention") and the second box ("Detection") is deterrence. Deterrence may be defined as the modification of behaviour through the threat of sanctions. Deterrence controls such as surprise audits have been shown to be highly effective in practice in reducing fraud, yet they are used only infrequently in business today. Fraud is, in essence, a people problem and controls that seek to influence behaviour through the perception of detection are very important. Deterrence mechanisms are often poorly understood by directors and managers and so are frequently under-utilised. We look at this whole area and in particular the importance of the "perception of detection" concept in more detail in Chapter 8 of the book.

4. Detection

The second box is labelled "Detection" and delegates are always very interested in this area of the fraud framework. This observation goes wider than delegates on my training courses however, as everyone that I have worked with in business in a forensic context has wanted to be able to detect fraud. Well, the first thing that I always say here is that fraud is in reality very difficult to detect! It is often carried out by individuals who are in senior positions or who have worked for an organisation for a long time and so have a detailed knowledge of the systems and of any control weaknesses. They are therefore in the ideal position to commit and conceal fraud. The purpose of detective controls is to reduce the exposure gap – the length of time from when a fraud starts to when the victim organisation finds out about it. The typical exposure gap in business will be around18 months to two years. This often comes as quite a shock to delegates and it illustrates well

the practical difficulties in uncovering fraudulent schemes. This is an area we will return to at length later in Chapter 8.

5. Risk-Based Approach

I always suggest to my delegates that the most important part of the diagram is not the boxes at all but rather the background, which is denoted by the word "Risk". The "risk" framework provides the entire context within which fraud has to be managed. The delegates will broadly agree with me on this, which is always encouraging. However, when I ask how many of the organisations represented in the room have taken the time and effort to identify, analyse, assess and document their fraud risk exposure, very few of my delegates ever put their hands up. This remains true even today. It is disappointing and a little surprising given the greater awareness of the importance of risk management principles today. Risk is dynamic, it changes all the time. This is particularly true of a threat like fraud and yet most businesses seem not to be aware of the importance of a regular, systematic assessment of fraud risk in order for the mitigating controls and procedures to be periodically updated and therefore to remain adequate. Specific fraud risks change all the time. If anti-fraud controls remain the same, then over time there is a widening gap between risk and controls. There is danger for all organisations in this widening gap.

Risk principles underpin this book and we will return frequently to the risk-based approach in tackling fraud frequently in the coming Chapters.

Summary – Five Key Learning Points for Directors and Managers

This Chapter on responsibility provides the overall framework that will enable directors and managers to deal with the threats of fraud in an effective and proportionate way. Before looking at some of the detailed controls and procedures in later Chapters it is worth pausing a moment and looking at the key lessons learned. There are five key learning points as follows:

✓ Remember the Responsibility Framework and the associated triangle diagram. All risks and controls can be fitted into this framework. Ultimate responsibility for managing risk resides with the board and senior managers. This is devolved to departmental heads and line managers who become effectively the point men and women in your organisation in relation to risk and controls. To make the whole thing work, the framework is underpinned by everyone being aware of personal responsibility for risk and controls when carrying out their work.

✓ Carry out regular fraud risk assessment (or risk profiling) exercises. Risk must be assessed and prioritised if it is to be managed effectively. Without assessing risk it will be impossible to design proportionate controls to manage your fraud threats effectively.

✓ Make sure that everything done to manage fraud risk is evidence-based. This means that the fraud risk assessment must be documented and also that all policies, procedures, training programmes etc. must exist and be updated regularly.

✓ Do not over-rely on traditional audit techniques for fraud prevention and detection. Be realistic in terms of the focus of external audit work and try to improve internal audit

capabilities through a combination of recruiting experts and investing in training programmes and/or modern detective tools.

✓ Take a strategic approach to the problem. Commit to a fraud risk management programme, be proactive and focus resources on the areas of prevention and deterrence. Have appropriate detective measures in place to reduce the exposure gap to a minimum and have access to investigation expertise, either external or in-house, to give assurance that potential future fraud events will be dealt with in an appropriate and timely manner.