CIMA

Chartered Institute of Management Accountants

Fraud risk management

A guide to good practice

Acknowledgements

This guide is based on the first edition of *Fraud Risk Management: A Guide to Good Practice*. The first edition was prepared by a Fraud and Risk Management Working Group, which was established to look at ways of helping management accountants to be more effective in countering fraud and managing risk in their organisations.

This second edition of *Fraud Risk Management: A Guide to Good Practice* has been updated by Helenne Doody, a specialist within CIMA Innovation and Development. Helenne specialises in Fraud Risk Management, having worked in related fields for the past nine years, both in the UK and other countries. Helenne also has a graduate certificate in Fraud Investigation through La Trobe University in Australia and a graduate certificate in Fraud Management through the University of Teeside in the UK.

For their contributions in updating the guide to produce this second edition, CIMA would like to thank:

Martin Birch FCMA, MBA	Director – Finance and Information Management, Christian Aid.
Roy Katzenberg	Chief Financial Officer, RITC Syndicate Management Limited.
Judy Finn	Senior Lecturer, Southampton Solent University.
Dr Stephen Hill	E-crime and Fraud Manager, Chantrey Vellacott DFK.
Richard Sharp BSc, FCMA, MBA	Assistant Finance Director (Governance), Kingston Hospital NHS Trust.
Allan McDonagh	Managing Director, Hibis Europe Ltd.
Martin Robinson and Mia Campbell	on behalf of the Fraud Advisory Panel.

CIMA would like also to thank those who contributed to the first edition of the guide.

About CIMA
CIMA, the Chartered Institute of Management Accountants, is the only international accountancy body with a key focus on business. It is a world leading professional institute that offers an internationally recognised qualification in management accounting, with a full focus on business, in both the private and public sectors. With 164,000 members and students in 161 countries, CIMA is committed to upholding the highest ethical and professional standards of its members and students.

Contents

Introduction 5

1 **Fraud – its extent, patterns and causes** 7
1.1 What is fraud? 7
1.2 The scale of the problem 9
1.3 Which businesses are affected? 11
1.4 Why do people commit fraud? 13
1.5 Who commits fraud? 15
1.6 Summary 16

2 **Risk management – an overview** 17
2.1 What is risk management? 17
2.2 Corporate governance 17
2.3 The risk management cycle 19
2.4 Establish a risk management group and set goals 20
2.5 Identify risk areas 20
2.6 Understand and assess the scale of risk 20
2.7 Develop a risk response strategy 22
2.8 Implement the strategy and allocate responsibilities 22
2.9 Implement and monitor suggested controls 22
2.10 Review and refine and do it again 22
2.11 Information for decision making 22
2.12 Summary 23

3 **Fraud prevention** 24
3.1 A strategy to combat fraud 24
3.2 Developing a sound ethical culture 26
3.3 Sound internal control systems 32
3.4 Summary 36

4 **Fraud detection** 37
4.1 Detection methods 37
4.2 Indicators and warnings 39
4.3 Tools and techniques 41
4.4 Summary 43

5 **Responding to fraud** 44
5.1 Purpose of the fraud response plan 44
5.2 Corporate policy 44
5.3 Definition of fraud 45
5.4 Roles and responsibilities 45
5.5 The response 47
5.6 The investigation 48
5.7 Organisation's objectives with respect to dealing with fraud 50
5.8 Follow-up action 50
5.9 Summary 51

Appendices

Appendix 1 Fraud and the law . . . 52
Appendix 2 Examples of common types of internal fraud . . . 57
Appendix 3 Example of a risk analysis . . . 60
Appendix 4 A sample fraud policy . . . 61
Appendix 5 Sample whistleblowing policy . . . 62
Appendix 6 Examples of fraud indicators, risks and controls . . . 64
Appendix 7 A 16 step fraud prevention plan . . . 67
Appendix 8 Outline fraud response plan . . . 68
Appendix 9 Example of a fraud response plan . . . 69
Appendix 10 References and further reading . . . 77
Appendix 11 Listed abbreviations . . . 80

Figures

Figure 1 Types of internal fraud . . . 8
Figure 2 The fraud triangle . . . 13
Figure 3 The CIMA risk management cycle . . . 19
Figure 4 Anti-fraud strategy . . . 25
Figure 5 Ethics advice/services provided . . . 28
Figure 6 Methods of fraud detection . . . 37

Case Studies

Case study 1 Fraud doesn't involve just money . . . 10
Case study 2 Size really doesn't matter . . . 12
Case study 3 A breach of trust . . . 14
Case study 4 Management risk . . . 16
Case study 5 A fine warning . . . 35
Case study 6 Vet or regret? . . . 36
Case study 7 Tipped off . . . 38
Case study 8 Risk or returns . . . 42
Case study 9 Reporting fraud . . . 45
Case study 10 TNT roots our fraud . . . 48

Introduction

Periodically, the latest major fraud hits the headlines as other organisations sit back and watch, telling themselves that 'it couldn't happen here.' But the reality is that fraud can happen anywhere. While only relatively few major frauds are picked up by the media, huge sums are lost by all kinds of businesses as a result of the high number of smaller frauds that are committed.

Surveys are regularly carried out in an attempt to estimate the true scale and cost of fraud to business and society. Findings vary, and it is difficult to obtain a complete picture as to the full extent of the issue, but these surveys all indicate that fraud is prevalent within organisations and remains a serious and costly problem. The risks of fraud may only be increasing, as we see growing globalisation, more competitive markets, rapid developments in technology, and periods of economic difficulty.

Among other findings, the various surveys highlight that:

- organisations may be losing as much as 7% of their annual turnover as a result of fraud
- corruption is estimated to cost the global economy about $1.5 trillion each year
- only a small percentage of losses from fraud are recovered by organisations
- a high percentage of frauds are committed by senior management and executives
- greed is one of the main motivators for committing fraud
- fraudsters often work in the finance function
- fraud losses are not restricted to a particular sector or country
- the prevalence of fraud is increasing in emerging markets.

Despite the serious risk that fraud presents to business, many organisations still do not have formal systems and procedures in place to prevent, detect and respond to fraud. While no system is completely foolproof, there are steps which can be taken to deter fraud and make it much less attractive to commit. It is in assisting organisations in taking such steps that this guide should prove valuable.

The original guide to good practice was based on the work of CIMA's Fraud and Risk Management Working Group that was established as part of the Institute's response to the problem of fraud. Since the publication of the original guide, we have continued to see high profile accounting scandals and unacceptable levels of fraudulent behaviour. This second edition of the guide includes updates to reflect the many changes in the legal environment and governance agenda in recent years, aimed at tackling the ongoing problem of fraud.

The guide starts by defining fraud and giving an overview of the extent of fraud, its causes and its effects. The initial chapters of the guide also set out the legal environment with respect to fraud, corporate governance requirements and general risk management principles. The guide goes on to discuss the key components of an anti-fraud strategy and outlines methods for preventing, detecting and responding to fraud. A number of case studies are included throughout the guide to support the text, demonstrating real life problems that fraud presents and giving examples of actions organisations are taking to fight fraud.

Management accountants, whose professional training includes the analysis of information and systems, can have a significant role to play in the development and implementation of anti-fraud measures within their organisations. This guide is intended to help management accountants in that role and will also be useful to others with an interest in tackling fraud in their organisation.

The law relating to fraud varies from country to country. Where it is necessary for this guide to make reference to specific legal measures, this is generally to UK law, as it would be impossible to include references to the laws of all countries where this guide will be read. It is strongly advised that readers ensure they are familiar with the law relating to fraud in their own jurisdiction. Although some references may therefore not be relevant to all readers, the general principles of fraud risk management will still apply and organisations around the world are encouraged to take a more stringent approach to preventing, detecting and responding to fraud.

1 Fraud: its extent, patterns and causes

1.1 What is fraud?

Definition of fraud
The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. The legal definition varies from country to country, and it is only since the introduction of the Fraud Act in 2006, that there has been a legal definition of fraud in England and Wales.

Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another. Although definitions vary, most are based around these general themes.

Fraud and the law
Before the Fraud Act came into force, related offences were scattered about in many areas of the law. The Theft Acts of 1968 and 1978 created offences of false accounting, and obtaining goods, money and services by deception, and the Companies Act 1985 included the offence of fraudulent trading. This remains part of the Companies Act 2006. There are also offences of fraud under income tax and value-added tax legislation, insolvency legislation, and the common law offence of conspiracy to defraud.

The Fraud Act is not the only new piece of legislation. Over the last few years there have been many changes to the legal system with regard to fraud, both in the UK and internationally. This guide focuses mainly on UK requirements, but touches on international requirements that impact UK organisations. In the UK, the Companies Act and the Public Interest Disclosure Act (PIDA) have been amended and legislation such as the Serious Crimes Act 2007 and the Proceeds of Crime Act 2002 (POCA) have been introduced. Internationally the Sarbanes-Oxley Act 2002 (Sarbox) has been introduced in the United States (US), a major piece of legislation that affects not only companies in the US but also those in the UK and others based all over the globe. Further information on these pieces of legislation can be found in Appendix 1.

As well as updating the legislation in the UK, there have been, and will continue to be, significant developments in the national approach to combating fraud, particularly as we see implementation of actions resulting from the national Fraud Review. Appendix 1 gives further information on the Fraud Review. There are also many law enforcement agencies involved in the fight against fraud in the UK, including the Serious Fraud Office, the Serious Organised Crime Agency (SOCA), the Financial Services Authority (FSA), and Economic Crime Units within the police force.

Different types of fraud
Fraud can mean many things and result from many varied relationships between offenders and victims. Examples of fraud include:

- crimes by individuals against consumers, clients or other business people, e.g. misrepresentation of the quality of goods; pyramid trading schemes
- employee fraud against employers, e.g. payroll fraud; falsifying expense claims; thefts of cash, assets or intellectual property (IP); false accounting
- crimes by businesses against investors, consumers and employees, e.g. financial statement fraud; selling counterfeit goods as genuine ones; not paying over tax or National Insurance contributions paid by staff
- crimes against financial institutions, e.g. using lost and stolen credit cards; cheque frauds; fraudulent insurance claims
- crimes by individuals or businesses against government, e.g. grant fraud; social security benefit claim frauds; tax evasion
- crimes by professional criminals against major organisations, e.g. major counterfeiting rings; mortgage frauds; 'advance fee' frauds; corporate identity fraud; money laundering
- e-crime by people using computers and technology to commit crimes, e.g. phishing; spamming; copyright crimes; hacking; social engineering frauds.

This guide focuses on fraud against businesses, typically by those internal to the organisation. According to the Association of Certified Fraud Examiners (ACFE), there are three main categories of fraud that affect organisations. The first of these is asset misappropriations, which involves the theft or misuse of an organisation's assets. Examples include theft of plant, inventory or cash, false invoicing, accounts receivable fraud, and payroll fraud.

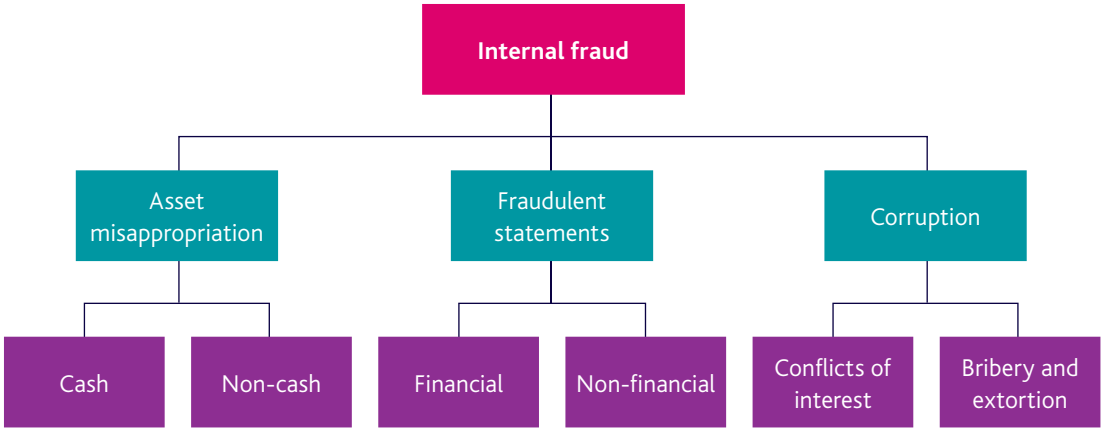
The second category of fraud is fraudulent statements. This is usually in the form of falsification of financial statements in order to obtain some form of improper benefit. It also includes falsifying documents such as employee credentials.

The final of the three fraud categories is corruption. This includes activities such as the use of bribes or acceptance of 'kickbacks', improper use of confidential information, conflicts of interest and collusive tendering. These types of internal fraud are summarised in Figure 1.

Surveys have shown that asset misappropriation is the most widely reported type of fraud in UK, although corruption and bribery are growing the most rapidly.

Further information on common types of internal fraud, and methods by which they may be perpetrated, is included in Appendix 2.

Figure 1 Types of internal fraud



1.2 The scale of the problem

There have been many attempts to measure the true extent of fraud, but compiling reliable statistics around fraud is not easy. As one of the key aspects of fraud is deception, it can be difficult to identify and survey results often only reflect the instances of fraud that have actually been discovered. It is estimated that the majority of frauds go undetected and, even when a fraud has been found, it may not be reported. One reason for this may be that a company that has been a victim of fraud does not want to risk negative publicity. Also, it is often hard to distinguish fraud from carelessness and poor record keeping.

Although survey results and research may not give a complete picture, the various statistics do offer a useful indication as to the extend of the problem. There can be no doubt that fraud is prevalent within organisations and remains a serious issue. PricewaterhouseCooper's *Global Economic Crime Survey* (PwC's survey) in 2007 found that over 43% of international businesses were victims of fraud during the previous two years. In the UK, the figures were higher than the global average, with 48% of companies having fallen victim to fraud.

Some surveys put the figures much higher. For example, during 2008, Kroll commissioned the Economist Intelligence Unit (EIU) to poll nearly 900 senior executives across the world. The EIU found that 85% of companies had suffered from at least one fraud in the past three years[1]. This figure had risen from 80% in a similar poll in 2007. KPMG's *Fraud Barometer,* which has been running since 1987, has also shown a considerable increase in the number of frauds committed in the UK in recent years, including a 50% rise in fraud cases in the first half of 2008.

According to the UK report of PwC's survey, the average direct loss per company over a two year period as a result of fraud has risen to £1.75 million, increasing from £0.8 million in the equivalent 2005 survey. These figures exclude undetected losses and indirect costs to the business such as management costs or damage to reputation, which can be significant. Management costs alone were estimated to be on average another £0.75 million. Participants of the ACFE *Report to the Nation* 2008 (ACFE report) estimated that organisations lose 7% of their annual revenues to fraud.

It is difficult to put a total cost on fraud, although many studies have tried to. For example an independent report by the Association of Chief Police Officers (the ACPO) in 2007 revealed that fraud results in losses of £20 billion each year in the UK. The World Bank has estimated that the global cost of corruption and bribery is about 5% of the value of the world economy or about $1.5 trillion per year. It is thought that these estimates are conservative, and they also exclude other types of fraud such as misappropriation of assets.

While it may be impossible to calculate the total cost of fraud, it is said to be more significant than the total cost of most other crimes. According to the Attorney General in the UK, fraud is an area of crime which is second only to drug trafficking in terms of causing harm to the economy and society[2].

1 Kroll Global Fraud Report, Annual Edition 2008/2009
2 Attorney General's interim report on the government's Fraud Review, March 2006

Fraud is often mistakenly considered a victimless crime. However, fraud can have considerable social and psychological effects on individuals, businesses and society. For example, when a fraud causes the collapse of a major company, numerous individuals and businesses can be affected. In addition to the company's own employees, employees of suppliers can be affected by the loss of large orders, and other creditors, such as banks, can be indirectly affected by huge losses on loans. Consumers have to pay a premium for goods and services, in order to compensate for the costs of fraud losses and for money spent on investigations and additional security.

Taxpayers also suffer due to reduced payments of corporation tax from businesses that have suffered losses. Fraud drains resources, affects public services and, perhaps of more concern, may fund other criminal and terrorist activity. According to the Fraud Review, fraud is a major and growing threat to public safety and prosperity. Case study 1 demonstrates just how much of a threat fraud can be to public safety and that there truly are victims of fraud.

Case study 1

Fraud doesn't just involve money

Counterfeiting is one example of fraud that can have extremely serious consequences. Technology is ever improving, making it easier for counterfeiters to produce realistic looking packaging and fool legitimate wholesalers and retailers. Counterfeiting is a potentially lucrative business for the fraudster, with possibilities of large commercial profits, and it is a problem affecting a wide range of industries including wines and spirits, pharmaceuticals, electrical goods, and fashion. However, there are often many victims affected by such a fraud and not just the business that has been duped or had their brand exploited. For some, the outcome of counterfeiting goes way beyond financial losses and can even be fatal:

- In late 2006, 14 Siberian towns declared a state of emergency due to mass poisonings caused by fake vodka. Around 900 people were hospitalised with liver failure after drinking industrial solvent that was being sold as vodka. This is not a one off problem and sales of fake alcohol have been known to kill people.

- Also in 2006, a counterfeit product did result in more tragic consequences. At least 100 children died after ingesting cough syrup that had been mixed with counterfeit glycerine. The counterfeit compound, actually a dangerous solvent, had been used in place of more expensive glycerine. The manufacturing process had been sourced to China and the syrup passed through trading companies in Beijing and Barcelona before reaching its final destination in Panama. The certificate attesting to the product's purity was falsified and not one of the trading companies tested the syrup to confirm its contents along the way. It is thought that the number of deaths is likely to be much higher than the 100 cases that have been confirmed.

1.3 Which businesses are affected?

Fraud is an issue that all organisations may face regardless of size, industry or country. If the organisation has valuable property (cash, goods, information or services), then fraud may be attempted. It is often high profile frauds in large multi-national organisations that are reported on in the media and smaller organisations may feel they are unlikely to be a target of fraudsters. However, according to the ACFE report, small businesses (classified as those with less than 100 employees) suffer fraud more frequently than large organisations and are hit by higher average losses. When small companies are hit by large fraud losses, they are less likely to be able to absorb the damage than a larger company and may even go out of business as a result.

The results of PwC's survey showed that companies reporting fraud were spread across many industries, with at least a quarter of the respondents in any one industry suffering from fraudulent incidents. Industries suffering the highest average losses were insurance and industrial manufacturing. Losses in the financial services industry, a sector frequently in the press and one with which fraud is often associated, were actually below average. Even not-for-profit organisations are not immune to fraud, with government institutions and many charities falling victim to unscrupulous fraudsters. As one director working in the international development and aid sector has pointed out, 'In my sector, fraud is not a possibility, it is a reality and we are always dealing with a number of suspicious incidents on a more or less permanent basis.'

PwC's survey also revealed that incidences of fraud were highest in companies in North America, Africa and Central and Eastern Europe (CEE), where more than half of the companies reported fraud. It was lowest in the Western European region, although the UK was much higher than the average for this region, with levels of fraud similar to those in CEE. The EIU poll commissioned by Kroll in 2007 found that respondents in countries such as India and China have seen a significant increase in the prevalence of corporate fraud in the last three years and this trend is likely to increase in businesses operating in emerging markets[3].

Although fraud is prevalent across organisations of all sizes and in all sectors and locations, research shows that certain business models will involve greater levels of fraud risk than others. The control environment should be adjusted to fit with the degree of risk exposure. Further guidance on risk assessment and controls is given in later chapters.

3 Kroll Global Fraud Report, Annual Edition 2007/2008

Case study 2

Size really doesn't matter

From a family affair...
A member of a small family business in Australia committed a $2m fraud, costing profits, jobs and a great deal of trust. The business owners became suspicious when they realised that their son in law used the company diesel card to buy petrol for his own car. On closer scrutiny, they soon uncovered a company cheque for $80,000 made payable to the son in law's personal account. BDO's Brisbane office discovered that the cheque and the fuel were just the tip of a vast iceberg. The company's complex accounts system allowed the son in law to disguise cheques payable to himself as creditor payments. He then became a signatory and took ever larger cheques. He claimed that the poor cash flow was due to losses in one particular division which the family therefore closed, creating redundancies and losing what was in truth a successful business. The costs of inefficient accounting systems and undue trust can be massive. Every business should protect itself with thorough controls and vigilance.

Adapted from '*FraudTrack 5 Fraud: A Global Challenge*' published by BDO Stoy Hayward

...to a major corporate scandal
WorldCom filed for bankruptcy protection in June 2002. It was the biggest corporate fraud in history, largely a result of treating operating expenses as capital expenditure. WorldCom (now renamed MCI) admitted in March 2004 that the total amount by which it had misled investors over the previous 10 years was almost US$75 billion (£42 billion) and reduced its stated pre-tax profits for 2001 and 2002 by that amount. WorldCom stock began falling in late 1999 as businesses slashed spending on telecom services and equipment. A series of debt downgrades raised borrowing costs for the company, struggling with about US$32 billion in debt. WorldCom used accounting tricks to conceal a deteriorating financial condition and to inflate profits.

Former WorldCom chief executive Bernie Ebbers resigned in April 2002 amid questions about US$366 million in personal loans from the company and a federal probe of its accounting practices. Ebbers was subsequently charged with conspiracy to commit securities fraud and filing misleading data with the Securities and Exchange Commission (SEC) and was sentenced to 25 years in prison. Scott Sullivan, former Chief Financial Officer, pleaded guilty to three criminal charges and was sentenced to five years in prison. Ultimately, losses to WorldCom shareholders were close to US$180 billion and the fraud also resulted in the loss of 17,000 jobs. The SEC said that WorldCom had committed 'accounting improprieties of unprecedented magnitude' – proof, it said, of the need for reform in the regulation of corporate accounting.

Adapted from *CIMA Official Learning System, Management Accounting Risk and Control Strategy*

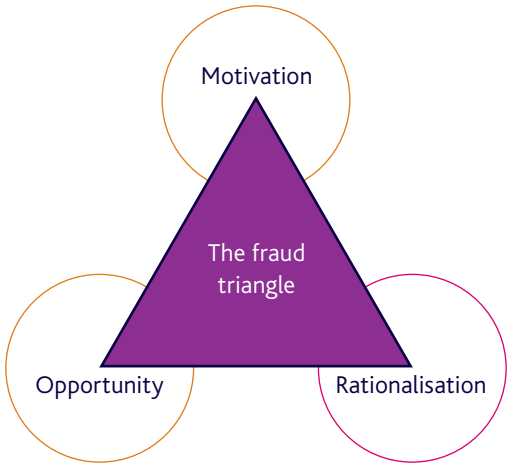
1.4 Why do people commit fraud?

There is no single reason behind fraud and any explanation of it needs to take account of various factors. Looking from the fraudster's perspective, it is necessary to take account of:

- motivation of potential offenders
- conditions under which people can rationalise their prospective crimes away
- opportunities to commit crime(s)
- perceived suitability of targets for fraud
- technical ability of the fraudster
- expected and actual risk of discovery after the fraud has been carried out
- expectations of consequences of discovery (including non-penal consequences such as job loss and family stigma, proceeds of crime confiscation, and traditional criminal sanctions)
- actual consequences of discovery.

A common model that brings together a number of these aspects is the Fraud Triangle. This model is built on the premise that fraud is likely to result from a combination of three factors: motivation, opportunity and rationalisation.

Figure 2 The fraud triangle



Motivation

In simple terms, motivation is typically based on either greed or need. Stoy Hayward's (BDO) most recent *FraudTrack* survey found that greed continues to be the main cause of fraud, resulting in 63% of cases in 2007 where a cause was cited. Other causes cited included problems from debts and gambling. Many people are faced with the opportunity to commit fraud, and only a minority of the greedy and needy do so. Personality and temperament, including how frightened people are about the consequences of taking risks, play a role. Some people with good objective principles can fall into bad company and develop tastes for the fast life, which tempts them to fraud. Others are tempted only when faced with ruin anyway.

Opportunity

In terms of opportunity, fraud is more likely in companies where there is a weak internal control system, poor security over company property, little fear of exposure and likelihood of detection, or unclear policies with regard to acceptable behaviour. Research has shown that some employees are totally honest, some are totally dishonest, but that many are swayed by opportunity.

Rationalisation

Many people obey the law because they believe in it and/or they are afraid of being shamed or rejected by people they care about if they are caught. However, some people may be able to rationalise fraudulent actions as:

- necessary – especially when done for the business
- harmless – because the victim is large enough to absorb the impact
- justified – because 'the victim deserved it' or 'because I was mistreated.'

Case study 3

A breach of trust

A good example of the fraud triangle in practice is the highly publicised case of the secretary that stole over £4.3 million from her bosses at Goldman Sachs.

Motivation

There were some suggestions that Joyti De-Laurey originally started down her fraudulent path because of financial difficulties she found herself in before starting work at the investment bank. De-Laurey had previously run her own sandwich bar business, but it was closed down due to insufficient finances. According to her defence, De-Laurey's 'first bitter experience of financial turmoil coincided with a novel introduction to a Dallas-type world where huge, unthinkable amounts of money stared her in the face, day in and day out.'

The motive behind the fraud was primarily greed though, with De-Laurey spending her ill gotten gains on a luxury lifestyle, including villas, cars, jewellery, designer clothes and first class holidays. De-Laurey has even admitted that she did not steal because she needed to, but because she could. She explained that she first started taking money simply to find out if she could get away with it. She says that it then became 'a bit addictive' and that she 'got a huge buzz from knowing they had no idea what I was doing.'

Opportunity

In terms of opportunity, De-Laurey's bosses trusted her and held her in high regard. She had proved herself indispensable, on both business and personal fronts, and was given access to their cheque books in order to settle their domestic bills and personal finances.

A little over a year after starting at Goldman Sachs, De-Laurey began forging her bosses' signatures on personal cheques to make payments into her own accounts. Realising she had got away with it, De-Laurey continued to steal money by issuing forged cheques and making false money transfers. Before long she was forging signatures on a string of cash transfer authorities, siphoning off up to £2.5 million at a time from supposedly secure New York investments.

Rationalisation

De-Laurey was able to rationalise her actions by convincing herself that she had earned the money she stole. De-Laurey believed that she deserved the plundered amounts as a just reward for her dedication, discretion and loyalty, and claims that she had the consent of her bosses to take money in return for her 'indispensable services'. The fact that they were so rich they did not even notice the money was missing, only served to fuel De-Laurey's fraudulent activities. She justified her actions through the belief that her bosses had cash to spare. According to De-Laurey; 'They could afford to lose that money.'

Caught out

After four years of siphoning off vast amounts of money, De-Laurey was eventually caught when her boss at the time decided to make a six-figure donation to his former college. He took a look at his bank accounts to see if he could cover the donation and was surprised to find the balance on the accounts so low. He investigated further and realised that large sums had been transferred to an unknown account. De-Laurey was the obvious suspect. By this time, De-Laurey had actually stolen around £3.3 million from this particular boss.

De-Laurey was the first woman in the UK to be accused of embezzling such a large sum and, after a long and high profile trial in 2004, she was sentenced to seven years imprisonment.

Various sources including *The Guardian, The Times, The Independent* and the *BBC News*

One of the most effective ways to tackle the problem of fraud is to adopt methods that will decrease motive or opportunity, or preferably both. Rationalisation is personal to the individual and more difficult to combat, although ensuring that the company has a strong ethical culture and clear values should help. These methods and principles are developed further in later chapters of this guide.

1.5 Who commits fraud?

Different types of fraudster
Fraudsters usually fall into one of three categories:

1 Pre-planned fraudsters, who start out from the beginning intending to commit fraud. These can be short-term players, like many who use stolen credit cards or false social security numbers; or can be longer-term, like bankruptcy fraudsters and those who execute complex money laundering schemes.

2 Intermediate fraudsters, who start off honest but turn to fraud when times get hard or when life events, such as irritation at being passed over for promotion or the need to pay for care for a family member, change the normal mode.

3 Slippery-slope fraudsters, who simply carry on trading even when, objectively, they are not in a position to pay their debts. This can apply to ordinary traders or to major business people.

In 2007, KPMG carried out research on the *Profile of a Fraudster* (KPMG survey), using details of fraud cases in Europe, India, the Middle East and South Africa. The ACFE carried out similar research on frauds committed in the US. These surveys highlight the following facts and figures in relation to fraudsters:

- perpetrators are typically college educated white male
- most fraudsters are aged between 36 and 55
- the majority of frauds are committed by men
- median losses caused by men are twice as great as those caused by women
- a high percentage of frauds are committed by senior management (including owners and executives)
- losses caused by managers are generally more than double those caused by employees
- average losses caused by owners and executives are nearly 12 times those of employees
- longer term employees tend to commit much larger frauds
- fraudsters most often work in the finance department, operations/sales or as the CEO.

The ACFE report also found that the type of person committing the offence depends on the nature of the fraud being perpetrated. Employees are most likely to be involved in asset misappropriation, whereas owners and executives are responsible for the majority of financial statement frauds. Of the employees, the highest percentage of schemes involved those in the accounting department. These employees are responsible for processing and recording the organisation's financial transactions and so often have the greatest access to its financial assets and more opportunity to conceal the fraud.

Case study 4

Management risk

In 2007, a major British construction firm suffered from extensive fraud committed by management at one of its subsidiaries. Accounting irregularities dating back to 2003 were said to include systematic misrepresentation of production volumes and sales by a number of senior figures at the division. Management at the subsidiary attempted to cover their behaviour by selling materials at a discounted price and the fraud went undetected for several years despite internal and external audits. The irregularities were eventually uncovered by an internal team sent to investigate a mismatch between orders and sales.

Following an initial internal investigation, a team of external experts and the police were brought in to identify the full extent of malpractice. The investigation found that the organisation was defrauded of nearly £23 million, but the fraud was said to cost the company closer to £40 million due to the written down value of the business and factoring in the cost of the investigation. The managing director of the subsidiary was dismissed, another manager faced disciplinary action and five others left before disciplinary proceedings could be commenced. Civil proceedings were ruled out on the basis that losses were unlikely to be recovered. Operations at the centre of the incident had to be temporarily closed and more than 160 jobs were cut at the business.

In addition to individual fraudsters, there has also been an increase in fraud being committed by gangs of organised criminals. Examples include false or stolen identities being used to defraud banks, and forms of e-fraud exploiting the use of internet by commercial businesses. SOCA is responsible for responding to such threats, with the support of the victim organisations.

1.6 Summary

A major reason why people commit fraud is because they are allowed to do so. There are a wide range of threats facing businesses. The threat of fraud can come from inside or outside the organisation, but the likelihood that a fraud will be committed is greatly decreased if the potential fraudster believes that the rewards will be modest, that they will be detected or that the potential punishment will be unacceptably high.

The main way of achieving this must be to establish a comprehensive system of control which aims to prevent fraud, and where fraud is not prevented, increases the likelihood of detection and increases the cost to the fraudster.

Later chapters of this guide set out some of the measures which can be put in place to minimise fraud risks to the organisation. Before looking specifically at fraud risk, the guide considers risk management in general.

2 Risk management – an overview

2.1 What is risk management?

Risk management is defined as the 'process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives' *(CIMA Official Terminology, 2005)*.

For an organisation, risks are potential events that could influence the achievement of the organisation's objectives. Risk management is about understanding the nature of such events and, where they represent threats, making positive plans to mitigate them. Fraud is a major risk that threatens the business, not only in terms of financial health but also its image and reputation.

This guide is primarily focused on managing the risk of fraud, but first, this chapter looks at more general aspects of risk management and corporate governance.

2.2 Corporate governance

Risk management is an increasingly important process in many businesses and the process fits in well with the precepts of good corporate governance. In recent years, the issue of corporate governance has been a major area for concern in many countries. In the UK, the first corporate governance report and code of best practice is considered to be the Cadbury Report in 1992, which was produced in response to a string of corporate collapses. There have been a number of reports since, covering provisions around areas such as executive remuneration, non-executive directors, and audit committees. The principles of these various reports have been brought together to form the Combined Code on Corporate Governance (Combined Code).

The Combined Code was first introduced in 1998 and among other matters, calls for boards to establish systems of internal control and to review the effectiveness of these systems on a regular basis. UK listed companies are required to provide a statement in their annual reports confirming that they comply with the Combined Code, and where they do not, they must provide an explanation for departures from it (the 'comply or explain' principle). The assessment of internal controls should be included in the report to shareholders. The Combined Code is reviewed regularly and the most recent version was published in June 2008.

Following the original introduction of the Combined Code, the Turnbull Committee was set up to issue guidance to directors on how they should assess and report on their review of internal controls. The Turnbull Committee made it clear that establishment of embedded risk management practices is key to effective internal control systems. The Turnbull guidance was first published in 1999 and revised in 2005. In the revised report (sometimes referred to as Turnbull 2) there is now a requirement for directors to give explicit confirmation that any significant failings or weaknesses identified from the review of effectiveness of internal controls have been, or are being, remedied.

The Financial Reporting Council is responsible for maintaining and reviewing the Combined Code, although the Combined Code is annexed to the rules of the UK Listing Authority, which is part of the FSA. The FSA is responsible for ensuring that listed companies provide the appropriate 'comply or explain' statement in their annual report. While the guidance is generally applicable to listed companies, the principles are relevant to all organisations and have been widely used as a basis for codes of best practice in the public and not-for-profit sectors. Fraud risk management practices are developing along the same lines.

Many other countries have also produced reports on corporate governance, usually accompanied by codes of best practices. For example, South Africa has had the King Report (version I and now II) since 1994, Malaysia has had its Code of Corporate Governance in place since 2000 and Sri Lanka issued the Rules on Corporate Governance as part of its Listing Rules in January 2007.

Corporate governance requirements in the US are now largely set out within the Sarbox legislation, further details on which are provided at Appendix 1. As previously mentioned, these requirements extend beyond the US, capturing any company that is SEC listed and its subsidiaries. Some other countries have also introduced a statutory approach to corporate governance, such as that in the US, although none are currently as comprehensive. A number of international organisations have also launched guidelines and initiatives on corporate governance, including the Organisation for Economic Co-operation and Development (OECD) and the European Commission.

An example of a growing area of corporate governance is IT governance, which has developed in light of rapid and continuing advances in information technology. The following box gives more information on IT governance.

IT Governance

IT governance is about ensuring that the organisation's IT systems support and enable achievement of the organisation's strategies and objectives. It encompasses leadership, organisational structures, businesses processes, standards and compliance.

There are five specific drivers for organisations to adopt IT governance strategies:

- regulatory requirements e.g. IT governance is covered by the Combined Code and Turnbull guidance in the UK
- increasing intellectual capital value that the organisation has at risk
- alignment of technology with strategic organisational goals
- complexity of threats to information security
- increase in the compliance requirements of information and privacy-related regulation.

A key benefit of an effective, integrated IT governance framework is the integration of IT into the strategic and overall operational approach of an organisation. There are a series of international Information Security (IS) standards that provide guidance on implementing an effective IT governance framework, known as the ISO 27000 series. For example, ISO/IEC 27001 defines a set of IS management requirements in order to help organisations establish and maintain an IS management system.

The standards apply to all types of organisation regardless of size or sector. They are particularly suitable where the protection of information is critical to the business, for example in the finance, health and public sectors, and for organisations which manage information on behalf of others, such as IT outsourcing companies.

ISACA also offers a series of IS standards and certification. ISACA is a leading global association in the IT governance and control field. With a network across more than 160 countries, its IS standards are followed by practitioners worldwide.

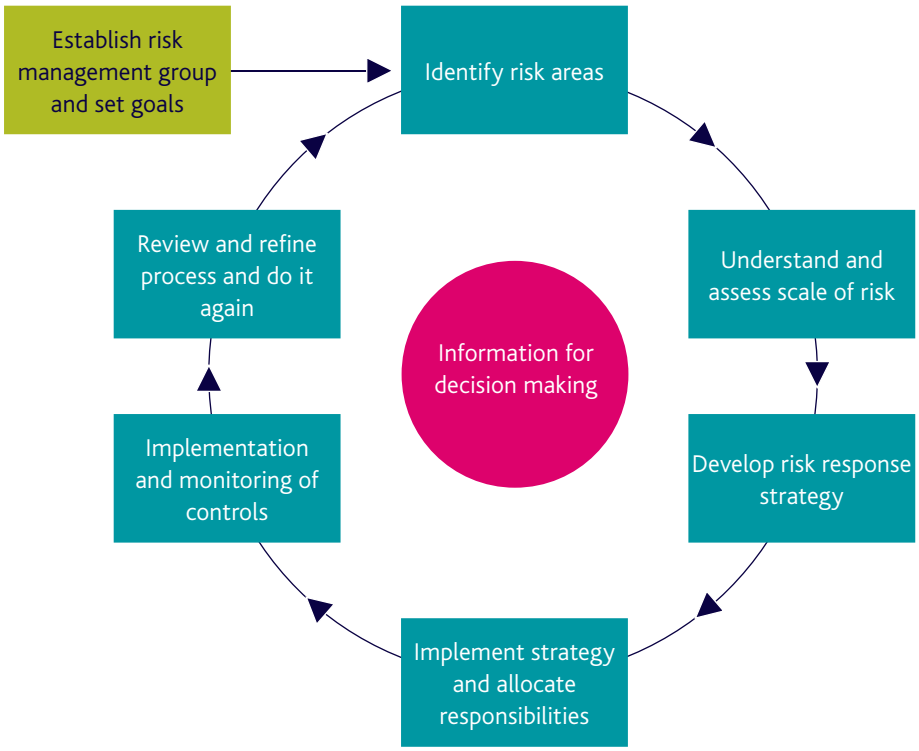
Controls assurance
Controls assurance is the process whereby controls are reviewed by management and staff. There are various ways to conduct these exercises, from highly interactive workshops based on behavioural models at one end of the spectrum to pre-packaged self audit internal control questionnaires at the other. These models all include monitoring and risk assessment among their principal components.

2.3 The risk management cycle

The risk management cycle is an interactive process of identifying risks, assessing their impact, and prioritising actions to control and reduce risks. A number of iterative steps should be taken:

1 Establish a risk management group and set goals.
2 Identify risk areas.
3 Understand and assess the scale of risk.
4 Develop a risk response strategy.
5 Implement the strategy and allocate responsibilities.
6 Implement and monitor the suggested controls.
7 Review and refine the process and do it again.

Figure 3 The CIMA risk management cycle



2.4 Establish a risk management group and set goals

A risk management group should be established whose task it is to facilitate and co-ordinate the overall risk management process. Possible members of the group could include a chief risk officer, a non executive director, finance director, internal auditor, heads of planning and sales, treasurer and operational staff. Depending on the size and nature of the organisation, the risk management group may be in the form of a committee who meet from time to time.

The risk management group will promote the understanding and assessment of risk, and facilitate the development of a strategy for dealing with the risks identified. They may also be responsible for conducting reviews of systems and procedures to identify and assess risks faced by the business, which include the risk of fraud, and introducing the controls that are best suited to the business unit. However, line managers and their staff may also be involved in the risk identification and assessment process, with the risk management group providing guidance.

2.5 Identify risk areas

Each risk in the overall risk model should be explored to identify how it potentially evolves through the organisation. It is important to ensure that the risk is carefully defined and explained to facilitate further analysis.

The techniques of analysis include:

- workshops and interviews
- brainstorming
- questionnaires
- process mapping
- comparisons with other organisations
- discussions with peers.

2.6 Understand and assess the scale of risk

Once risks have been identified, an assessment of possible impact and corresponding likelihood of occurrence should be made using consistent parameters that will enable the development of a prioritised risk analysis. In the planning stage, management should agree on the most appropriate definition and number of categories to be used when assessing both likelihood and impact.

The assessment of the impact of the risk should not simply take account of the financial impact but should also consider the organisation's viability and reputation, and recognise the political and commercial sensitivities involved. The analysis should either be qualitative or quantitative, and should be consistent to allow comparisons. The qualitative approach usually involves grading risks in high, medium and low categories.

Impact

The assessment of the potential impact of a particular risk may be complicated by the fact that a range of possible outcomes may exist or that the risk may occur a number of times in a given period of time. Such complications should be anticipated and a consistent approach adopted which, for example, may seek to estimate a worst case scenario over, say, a 12 month time period.

Likelihood of occurrence

The likelihood of a risk occurring should be assessed on a gross, a net and a target basis.

The gross basis assesses the inherent likelihood of the event occurring in the absence of any processes which the organisation may have in place to reduce that likelihood.

The net basis assesses the likelihood, taking into account current conditions and processes to mitigate the chance of the event occurring.

The target likelihood of a risk occurring reflects the risk appetite of the organisation.

Where the net likelihood and the target likelihood for a particular risk differ, this would indicate the need to alter the risk profile accordingly.

It is common practice to assess likelihood in terms of:
- high – probable
- moderate – possible
- low – remote.

An example of a risk analysis is contained in Appendix 3. The resulting document is often referred to as a risk register. The overall risk registers at organisational and operational levels should include the risk of fraud being perpetrated. Some organisations also prepare detailed fraud risk registers that consider possible fraudulent activity. The fraud risk register often directs the majority of proactive fraud risk management work undertaken by an organisation.

Analysing fraud risks

Fraud risk is one component of operational risk. Operational risk focuses on the risks associated with errors or events in transaction processing or other business operations. A fraud risk review considers whether these errors or events could be the result of a deliberate act designed to benefit the perpetrator. As a result, fraud risk reviews should be detailed exercises conducted by teams combining in depth knowledge of the business and market with detailed knowledge and experience of fraud.

Risks such as false accounting or the theft of cash or assets need to be considered for each part of the organisation's business. Frequently, businesses focus on a limited number of risks, most commonly on third-party thefts. To avoid this, the risks should be classified by reference to the possible type of offence and the potential perpetrator(s).

Fraud risks need to be assessed for each area and process of the business, for example, cash payments, cash receipts, sales, purchasing, expenses, inventory, payroll, fixed assets and loans.

2.7 Develop a risk response strategy

Once the risks have been identified and assessed, strategies to deal with each risk identified can be developed by line management, with guidance from the risk management group.

Strategies for responding to risk generally fall into one of the following categories:

- risk retention (e.g. choosing to accept small risks)
- risk avoidance (e.g. stopping sale of certain products to avoid the risk to occurring)
- risk reduction (e.g. through implementing controls and procedures)
- risk transfer (e.g. contractual transfer of risk; transferring risks to insurers).

Before strategies are developed, it is necessary to establish the risk appetite of the organisation. Risk appetite is the level of risk that the organisation is prepared to accept and this should be determined by the board. The appetite for risk will influence the strategies to be developed for managing risk. It is worth noting that a board's risk appetite may vary for different types of risk and over time. For example, the board may have a low risk tolerance on compliance and regulatory issues, but be prepared to take significant strategic risks. The board may also reduce their risk appetite as the external environment changes, such as in times of recession.

2.8 Implement the strategy and allocate responsibilities

The chosen strategy should be allocated and communicated to those responsible for implementation. For the plan to be effective it is essential that responsibility for each specific action is assigned to the appropriate operational manager and that clear target dates are established for each action. It is also important to obtain the co-operation of those responsible for the strategy, by formal communication, seminars, action plans and adjustments to budgets.

2.9 Implement and monitor suggested controls

The chosen strategy may require the implementation of new controls or the modification of existing controls. Businesses are dynamic and the controls that are in place will need to be monitored to assess whether or not they are succeeding in their objectives. The risk management group should be empowered to monitor the effectiveness of the actions being taken in each specific area, as these can be affected by internal and external factors, such as changes in the marketplace or the introduction of new computer systems.

2.10 Review and refine and do it again

All of the elements outlined above form part of an iterative cycle where risk management is continually reviewed and developed. As the cycle continues, risk management should increasingly become embedded in the organisation so that it really becomes part of everyone's job.

2.11 Information for decision making

Risk management should form a key part of the organisation's decision-making process. Information is gathered at all stages of the risk management cycle and this information should be fed into the decision-making mechanisms.

For more information on risk management, please refer to CIMA's publication *Risk Management: A guide to good practice*.

2.12 Summary

There are risks in most situations. Risk management is an important element of corporate governance and every organisation should review their risk status and develop their approach as described in the CIMA Risk Management Cycle in 2.3 to 2.11 above.

Managing the risk of fraud is the same in principle as managing any other business risk. First, the potential consequences of fraud on the organisation need to be understood, using the principles set out in this chapter. The risks should then be reduced by developing and implementing an anti-fraud strategy across the organisation. This is best approached systematically, both at the organisational level, for example by using ethics policies and anti-fraud policies, and at the operational level, through introduction of controls and procedures. The following chapters expand on the fraud risk management process in the context of an anti-fraud strategy.

3 Fraud prevention

3.1 A strategy to combat fraud

Given the prevalence of fraud and the negative consequences associated with it, there is a compelling argument that organisations should invest time and resources towards tackling fraud. There is, however, sometimes debate as to whether these resources should be committed to fraud prevention or fraud detection.

Fraud prevention
Based on the earlier discussion around why people commit fraud, it would seem that one of the most effective ways to deal with the problem of fraud is to adopt methods that will decrease motive, restrict opportunity and limit the ability for potential fraudsters to rationalise their actions. In the case of deliberate acts of fraud, the aim of preventative controls is to reduce opportunity and remove temptation from potential offenders. Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

It is profitable to prevent losses, and fraud prevention activities can help to ensure the stability and continued existence of a business. However, based on recent surveys, many organisations do not have a formal approach to fraud prevention. Once a fraud has already occurred, the likelihood of recovering stolen funds from the perpetrator or through insurance is often relatively low. According to KPMG's survey in 2007, only 16% of organisations profiled were able to recover their losses. A number of others are still trying to recover stolen assets, but the process is often difficult and lengthy. At least half of the organisations have been unable to recover any assets at all. As such, it is preferable to try to prevent the loss from occurring in the first place and the old adage 'prevention is better than cure' certainly applies to fraud.

It is worth bearing in mind though, that fraud prevention techniques, while worth investing in, cannot provide 100% protection. It is difficult, if not impossible, to remove all opportunities for perpetrating fraud.

Fraud detection
As fraud prevention techniques may not stop all potential perpetrators, organisations should ensure that systems are in place that will highlight occurrences of fraud in a timely manner. This is achieved through fraud detection. A fraud detection strategy should involve use of analytical and other procedures to highlight anomalies, and the introduction of reporting mechanisms that provide for communication of suspected fraudulent acts. Key elements of a comprehensive fraud detection system would include exception reporting, data mining, trend analysis and ongoing risk assessment.

Fraud detection may highlight ongoing frauds that are taking place or offences that have already happened. Such schemes may not be affected by the introduction of prevention techniques and, even if the fraudsters are hindered in the future, recovery of historical losses will only be possible through fraud detection. Potential recovery of losses is not the only objective of a detection programme though, and fraudulent behaviour should not be ignored just because there may be no recovery of losses. Fraud detection also allows for the improvement of internal systems and controls. Many frauds exploit deficiencies in control systems. Through detection of such frauds, controls can be tightened making it more difficult for potential perpetrators to act.

Fraud prevention and fraud detection both have a role to play and it is unlikely that either will fully succeed without the other. Therefore, it is important that organisations consider both fraud prevention and fraud detection in designing an effective strategy to manage the risk of fraud.

An anti-fraud strategy

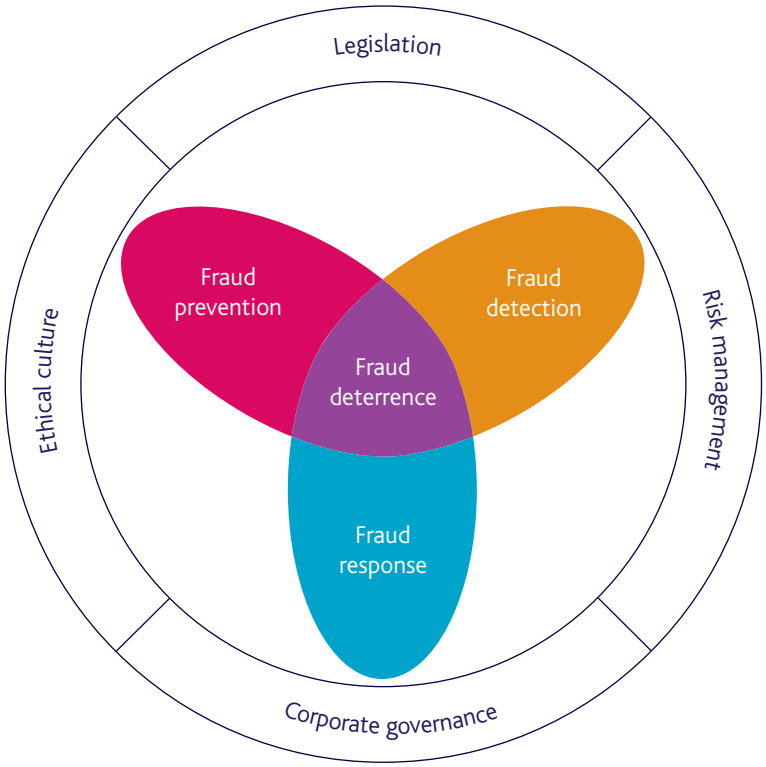
An effective anti-fraud strategy in fact has four main components:

- prevention
- detection
- deterrence
- response.

The following diagram summarises these components and the context within which an anti-fraud strategy sits.

It is clear from Figure 4 that the various elements of an effective anti-fraud strategy are all closely interlinked and each plays a significant role in combating fraud. Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organisation is actively fighting fraud and that procedures are in place to identify any illegal activity that has occurred. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud. Complementary detection controls should also be in place to counter the fact that the prevention controls may be insufficient in some cases.

Figure 4 Anti-fraud strategy



A consistent and comprehensive response to suspected and detected incidents of fraud is also important. This sends a message that fraud is taken seriously and that action will be taken against perpetrators. Each case that is detected and investigated should reinforce this deterrent and, therefore, act as a form of fraud prevention.

The various components of an effective anti-fraud strategy are discussed over the next few chapters. The remainder of this chapter examines some of the main preventative approaches which can be implemented to minimise the occurrence and cost of fraud within an organisation. These approaches are generic and can be applied, as appropriate, to different organisations and particular circumstances.

3.2 Developing a sound ethical culture

Attitudes within an organisation often lay the foundation for a high or low fraud risk environment. Where minor unethical practices may be overlooked (e.g. petty theft, expenses frauds), larger frauds committed by higher levels of management may also be treated in a similar lenient fashion. In this environment there may be a risk of total collapse of the organisation either through a single catastrophic fraud or through the combined weight of many smaller frauds.

Organisations which have taken the time to consider where they stand on ethical issues have come to realise that high ethical standards bring long term benefits as customers, suppliers, employees and the community realise that they are dealing with a trustworthy organisation. They have also realised that dubious ethical or fraudulent practices cause serious adverse consequences to the people and organisations concerned when exposed.

The definition of good ethical practice is not simple. Ideas differ across cultural and national boundaries and change over time. But corporate ethics statements need not be lengthy to be effective. The following is an example of guiding business principles that BT applies to all employees, agents, and others representing BT. These principles could form the basis of an ethics statement in an international environment.

BT's business principles

- **Legal**
  We will act within the law, our licensing/ authorisations obligations and any other regulations.
- **Compete fairly**
  Compete vigorously but fairly in our markets, being honest and trustworthy in all our dealings.
- **Inducements**
  Not offer or accept gifts, hospitality or other inducements which encourage or reward a decision, or engage in any form of bribery. Report and record any incident.
- **Conflicts**
  Avoid or declare conflicts of interest that may lead (or be seen to lead) to divided personal loyalties.
- **Commitments**
  Ensure others have confidence in the commitments we make on behalf of BT, and that agreements are suitably authorised.
- **Risks**
  Assess and manage risks to our business.
- **Assets**
  Protect our brand, physical, financial and intellectual assets.
- **Information**
  Protect the confidentiality of company, employee and customer information.
- **Communication**
  Be truthful, helpful and accurate in our communication.
- **Diversity**
  Treat all individuals fairly and impartially, without prejudice, and never tolerate harassment in any form.
- **Health and safety**
  Care for the health and safety of each other, our products and our operations.
- **Environment**
  Minimise the potential harmful effects of our activities on the environment.

Reproduced with kind permission of BT

Organisations which have created a positive ethical culture have normally either been driven by a committed chief executive or have been forced to do so because of incidents which caused, or almost caused, significant loss to the organisation.

With regards to establishing a sound ethical culture, CIMA recommends that organisations have:

- a mission statement that refers to quality or, more unusually, to ethics and defines how the organisation wants to be regarded externally
- clear policy statements on business ethics and anti-fraud, with explanations about acceptable behaviour in risk prone circumstances (a sample fraud policy is included at Appendix 4)
- a route through which suspected fraud can be reported
- a process of reminders about ethical and fraud policies – e.g. annual letter and/or declarations
- an aggressive audit process which concentrates on areas of risk
- management who are seen to be committed through their actions.

IFAC's Professional Accountants in Business (PAIB) Committee has produced guidance that focuses on the role of accountants in developing and promoting codes of conduct within their business (see Further Reading in Appendix 10 for more detail). CIMA members should also bear in mind the CIMA Code of Ethics for Professional Accountants, which sets out standards around ethical conduct and acting with integrity and objectivity, even in potentially difficult circumstances. For example, the CIMA Code of Ethics deals with safeguarding assets, potential conflicts, preparation and reporting of information, threats of financial self interest, inducements, and confidentiality. Members of other professional bodies are likely to be bound by similar codes.

A code of ethics or an anti-fraud policy is not sufficient to prevent fraud though. Ethical behaviour needs to be embedded within the culture of an organisation. Commitment from senior management and 'tone at the top' is key. Employees are more likely to do what they see their superiors doing than follow an ethics policy, and it is essential that management do not apply double standards.

To demonstrate commitment, resources should be allocated to communicating ethics and values to all employees, suppliers and business partners, and providing training programmes where necessary. Research by the Institute of Business Ethics (IBE) has demonstrated that, through helping to establish an ethical culture, there is a correlation between ethics training and improved financial performance[4]. However, a recent survey conducted by CIMA, in conjunction with the IBE, found that although most organisations have adopted a code of ethics, many are not backing up their written statements with action. Less than half of the respondents' organisations provide ethics training or a hotline for reporting unethical conduct, and only a few offer incentives for employees to uphold ethical standards. These results are summarised in Figure 5.

In addition to encouraging senior management to set ethical examples by their actions, organisations should ensure that senior management are committed to controlling the risks of fraud. Senior management should be assigned with responsibility for fraud prevention, as this sends a message to employees that the organisation is serious about fraud and ensures that tackling fraud will be considered at senior levels. Adherence to policies and codes should be regularly monitored and policed by appropriate people within

Figure 5 Ethics advice/services provided

Source: *Managing Responsible Business,* CIMA, 2008

the organisation (such as management and/or internal audit), and the documents themselves should also be regularly reviewed and amended.

Periodic assessment of fraud risk
In order to manage fraud risk, organisations should periodically identify the risks of fraud within their organisation, using the process set out in Chapter 2. Fraud risks should be identified for all areas and processes of the business and then be assessed in terms of impact and likelihood. In addition to the monetary impact, the assessment should consider non financial factors such as reputation.

An effective fraud risk assessment will highlight risks previously unidentified and strengthen the ability for timely prevention and detection of fraud. Opportunities for cost savings may also be identified as a result of conducting the fraud risk assessment.

Fraud risk training and awareness
Almost every time a major fraud occurs many people who were unwittingly close to it are shocked that they were unaware of what was happening. Therefore, it is important to raise awareness through a formal education and training programme as part of the overall risk management strategy. Particular attention should be paid to those managers and staff operating in high risk areas, such as procurement and bill paying, and to those with a role in the prevention and detection of fraud, for example human resources and staff with investigation responsibility.

There are arguments about how far training on fraud risk management should go within an organisation beyond the audit group – for example a question often raised is whether management and staff who have been trained in fraud prevention techniques will then use the knowledge to commit fraud. Fraud is often highlighted through a tip off and therefore it is essential that all employees are made aware of what constitutes fraud, how to identify fraudulent behaviour, and how to respond if they suspect or detect instances of fraud. There is advantage in covering the subject of fraud in generic terms, the corporate ethic, the audit approach and the types of checks and balances built into processes. Such training is more likely to decrease rather than increase the number of fraudulent incidents.

Opposing double standards

It is too often presumed that there should be one set of rules for ordinary people and another for their leaders. Such attitudes breed cynicism and resentment. Though there will be some valid exceptions, leaders must almost always live by the rules they impose on others. Amongst other things this means taking a firm line on fraud by senior executives.

Reproduced with kind permission of the Fraud Advisory Panel from its Ninth Annual Review 2006-2007
'Ethical behaviour is the best defence against fraud'

4 Does business ethic pay – revisited, IBE

Employees may be educated through a number of mediums, such as formal training sessions, group meetings, posters, employee newsletters, payroll bulletins or awareness pages on internal websites. Communication should be ongoing and a combination of methods is usually most successful. For example, the UK's National Health Service (NHS) uses several different media to raise fraud risk awareness, including a quarterly staff newsletter called *Insight* that covers topics such as training updates, fraud case studies, risk measurement and prosecution examples.

It is clear that spending money on preventing fraud brings many benefits – but the cost benefit analysis is not easy to construct. The downside risk of fraud prevention is that excessive and expensive controls may be created, which reduce efficiency and demotivate staff. However, the head of fraud investigation for a major bank made the following observation: 'A £1m increase in expenditure on fraud prevention has led to a £25m increase in profits.'

Reporting mechanisms and whistleblowing

Establishing effective reporting mechanisms is one of the key elements of a fraud prevention programme and can have a positive impact on fraud detection. Many frauds are known or suspected by people who are not involved. The challenge for management is to encourage these 'innocent' people to speak out – to demonstrate that it is very much in their own interest. Research by the IBE has shown that although one in four employees are aware of misconduct in the workplace, over half of those people stay silent[6].

In this area there are many conflicting emotions influencing the potential 'whistleblower':

- working group/family loyalties
- disinterest/sneaking admiration
- fear of consequences
- suspicion rather than proof.

The organisation's anti-fraud culture and reporting processes can be a major influence on the whistleblower, as it is often fear of the consequences that has the impact. To the whistleblower the impact of speaking out can be traumatic, ranging from being dismissed to being shunned by other employees.

Where fraud is committed by senior managers (and this can be as high as the chief executive), then the predicament faced by the whistleblower is exacerbated. And this is where management's greatest challenge lies – to convince staff that everyone is responsible for combating fraud and that the good health of the organisation, and potentially their future employment, could be at risk from fraud. Organisations that encourage openness and can overcome the culture of silence are likely to benefit in many ways (see box on page 31).

6 Speak Up Procedures (2007), IBE

Benefits of a culture that encourages whistleblowing

An organisation where the value of open whistleblowing is recognised will be better able to:

- deter wrongdoing
- pick up potential problems early
- enable critical information to get to the people who need to know and can address the issue
- demonstrate to stakeholders, regulators, and the courts that they are accountable and well managed
- reduce the risk of anonymous and malicious leaks
- minimise costs and compensation from accidents, investigations, litigation and regulatory inspections
- maintain and enhance its reputation.

Enlightened organisations implement whistleblowing arrangements because they recognise that it makes good business sense.

Reproduced with kind permission of BSI from
PAS 1998:2008 Whistleblowing Arrangements Code of Practice

In the UK, there is legislation protecting whistleblowers, known as PIDA. Further information on PIDA is given in Appendix 1. Other countries also have legislation protecting whistleblowers, for example this is covered by Sarbox in the US. Legal redress should be a last resort though, and organisations should strive for a culture that actively encourages people to speak up and challenge inappropriate behaviour.

Although PIDA exists to protect whistleblowers, there is no statutory requirement for a whistleblowing policy under the legislation. However, organisations are encouraged to develop a written policy statement, and corporate governance codes in the UK provide more direction on this. Under the Combined Code, listed companies are obliged to have whistleblowing arrangements or explain why they do not, and public bodies are expected to have a policy in place, which are assessed regularly as part of the external audit and review of local authorities and NHS bodies. Companies captured under Sarbox are also required to have whistleblowing arrangements. A sample whistleblowing policy can be found in Appendix 5.

The British Standards Institute (BSI) has recently published a Publicly Available Specification (PAS), developed by Public Concern at Work, that gives guidance on 'good practice for the introduction, revision, operation and review of effective whistleblowing arrangements' (PAS 1998:2008 Whistleblowing Arrangements Code of Practice). The nature of the whistleblowing arrangements will be determined by an organisation's size, structure, culture, nature of the risks that it faces and the legal framework in which it operates.

A confidential 24/7 hotline is said to be one of the best methods for reporting fraud. However, open channels of communication from employees to management are also essential in creating an environment that encourages fraud prevention and detection. An open and honest culture should improve morale among employees and give them the confidence to come forward with concerns.

Following up on disclosures is an important part of any whistleblowing arrangement. Employees are more likely to speak up if they know that something will be done about their concern. This is supported by the findings of the CIMA ethics survey referred to earlier. A small percentage of respondents had personally observed unethical conduct and most reported the wrongdoing when they came across it, but many were dissatisfied with the response. By not handling concerns in a satisfactory way, organisations risk losing the confidence of their employees and discouraging them from speaking up in the future. The survey highlighted that the most common reason for not reporting a concern was thinking that it would not make a difference.

Management has to be aware of the risk of anonymous and malicious accusations, but they cannot afford to ignore any report in case it is correct. They may wish to state in their policy that anonymous advice will be treated with extreme caution. Companies captured under Sarbox have no choice but to offer a facility for anonymous reporting. This can cause difficulty for organisations operating in Europe, as it may conflict with EU data protection rules, which state that personal data should only be collected fairly. The EU data protection authorities have issued guidance on this (*Guidance on Whistleblowing Schemes,* 2006) and information can also be obtained from Public Concern at Work.

3.3 Sound internal control systems

A strong system of internal controls is considered by the ACFE to be 'the most valuable fraud prevention device by a wide margin'. Having sound internal control systems is also a requirement under the Companies Act, Sarbox and various corporate governance codes.

Responsibility for internal control

Overall responsibility for the organisation's system of internal control must be at the highest level in the organisation. Under the Companies Act, directors are responsible for maintaining adequate accounting records. The Combined Code prescribes that 'the board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets'. This should include procedures designed to minimise the risk of fraud. As mentioned in the previous chapter, the board should satisfy itself that the system is effective and report that it has undertaken such a review to its shareholders. The Turnbull report provides guidance on how this should be achieved.

There is often an expectation that auditors have responsibility for fraud prevention and detection. While auditors doubtless have a role to play in fraud risk management, they do not have primary responsibility. This lies with management and those charged with governance of the organisation. International Standard on Auditing 240 (ISA 240) clarifies these responsibilities, an extract of which is included in the box below. ISA 240 has recently been revised and the redrafted standard is effective for audits of financial statements for periods beginning on or after 15 December 2008.

Although primary responsibility for fraud prevention and detection does not sit with the auditor, ISA 240 does call for auditors to include methods for identifying potential cases of fraud when planning and conducting the audit. It requires auditors to:

- discuss the risk of fraud with management and those charged with governance
- discuss with the audit team the susceptibility of the accounts to material misstatements due to fraud
- consider whether one or more fraud risk factors are present
- perform audit procedures to address the risk of management override
- test journal entries and review accounting estimates for bias
- understand the business rationale for transactions outside the normal course of business
- obtain representations from management
- bear in mind the implications for money laundering reporting (taking care not to tip off the client).

In addition to the international auditing standard, some countries also have their own auditing standards that give further direction on roles and responsibilities in relation to fraud. For example, in October 2002, the US issued Statement on Auditing Standards No. 99 *Consideration of Fraud in a Financial Statement Audit* (SAS 99), partly in response to accounting scandals such as Enron and WorldCom. SAS 99 is more prescriptive about the role of the auditor in preventing and detecting fraud and error than ISA 240 and was designed to create a substantial change in auditors' performance, thereby improving the likelihood that auditors will detect material misstatements due to fraud.

The requirements do not only affect auditors. Given the nature and extent of the new procedures in both ISA 240 and SAS 99, management should plan to provide auditors with more information and open themselves up to more extensive fraud detection procedures.

Extract from ISA 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements* (redrafted)

Responsibility for the prevention and detection of fraud

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment.

This involves a commitment to creating a culture of honesty and ethical behavior which can be reinforced by an active oversight by those charged with governance. In exercising oversight responsibility, those charged with governance consider the potential for override of controls or other inappropriate influence over the financial reporting process, such as efforts by management to manage earnings in order to influence the perceptions of analysts as to the entity's performance and profitability.

Responsibilities of the auditor

An auditor conducting an audit in accordance with ISAs is responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error... (O)wing to the inherent limitations of an audit, there is an unavoidable risk that some material misstatements of the financial statements will not be detected, even though the audit is properly planned and performed in accordance with the ISAs.

Internal control systems

An internal control system comprises all those policies and procedures that taken together, support an organisation's effective and efficient operation. Internal controls typically deal with factors such as approval and authorisation processes, access restrictions and transaction controls, account reconciliations, and physical security. These procedures often include the division of responsibilities and checks and balances to reduce risk. The following box gives an example of division of responsibilities within the purchasing process.

Division of responsibilities in the purchasing process

Ideally, the purchasing process would involve the following separate roles:

- the originator who specifies the goods or services and probably price
- the superior who approves the purchase
- the purchasing department who negotiate the best value through competitive quotations
- the recipient of goods or services who confirms that the invoice is in line with goods or services received
- the purchase ledger/accounting department who make entries in the accounts
- the treasury manager who ensures that payments are properly supported and in line with policy
- the management accountant who ensures that costs are in line with budgets/standards and purchase ledger payment statistics are in line with policy.

Segregation of duties is not always possible though, and it may be necessary to introduce additional management examination and control, including some form of internal audit as a regular feature.

The number and type of internal controls that an organisation can introduce will again depend on the nature and size of the organisations. Internal controls to minimise fraud should, where possible, address fraud red flags (see Chapter 4 and Appendix 6). Examples of the variety of such controls include:

- requiring multiple signatories on high value transactions (e.g. within a finance or procurement department)
- enforcing employees to take holiday (e.g. many employees in the banking sector must take a minimum of two weeks holiday in a given period)
- restricting belongings that can be brought into the office environment (e.g. many call centre employees are not allowed to take in pens, paper or mobile phones, and some organisations have restricted the use of USB sticks)
- conducting random searches of staff (e.g. in factories, distribution centres or retail outlets).

Wherever new internal control procedures are introduced, they should be documented clearly and simply, in order that any deviation can be identified. Internal controls should be regularly reviewed as part of the risk management process, and there should be continual improvement of controls in light of new risks, such as new markets and technologies, changes in structure, or innovative fraudsters. Not only does this reflect good practice, but it is also a requirement of the Combined Code and Sarbox. Ultimately, the internal control system should be embedded within the culture and operations of an organisation.

Case study 5

A fine warning

A major European banking group has suffered in more ways than one from having weak internal controls. In 2007, a senior employee at the bank was able to transfer £1.3 million out of client accounts without permission. This was possible because the bank did not have effective review processes in place for transactions over £10,000 and its checking procedures were unclear.

Not only did the organisation suffer from losses and reputational damage at the hand of the fraudster, but the bank was also fined £350,000 by the FSA because of its ineffective anti-fraud measures. The bank had been warned by the FSA in 2002 that its internal controls needed to be improved. However, no steps were made to change the systems in place. Following the fine in 2007, the bank strengthened its controls and now claims to be among the best in the industry.

This is the first fine that the FSA has issued against a private bank for weaknesses in anti-fraud controls but it is stepping up its game in this area and this should serve as a caution for other organisations. The FSA has warned that 'senior management must make sure their firms have robust systems and controls to reduce the risk of them being used to commit financial crime.'

Source: *Weak anti-fraud measures earn bank hefty fine,* CIMA Industry focus, 15 May 2007

Pre-employment screening

Pre-employment screening is the process of verifying the qualifications, suitability and experience of a potential candidate for employment. Techniques used include confirmation of educational and professional qualifications, verification of employment background, criminal history searches, and credit checks. For all screening, the organisation must obtain the individual's written permission and all documents must bear the individual's name.

Screening applicants should reduce the likelihood of people with a history of dishonest or fraudulent behaviour being given a role within the company, and is therefore an important fraud prevention procedure. A significant proportion of CVs contain serious discrepancies, and in fraud cases investigated, there are often signs in the employee's background that would have been a warning to a potential employer had screening been conducted. Research has also shown that employers who conduct pre-employment screening experience fewer cases of fraud by employees.

At a minimum, organisations should consider screening for cash handling positions, senior management posts and other trusted positions such as treasury, accounts payable, and security. Screening should also not be limited to new joiners. An organisation should run checks before offering promotions and secondments into more senior or sensitive positions.

Organisations should also never assume that agency staff have been properly vetted by the contracting agency. As is demonstrated by the following case study, a recruitment agency's screening process cannot always be relied upon.

Case study 6

Vet or regret?

Without a trace

A finance house needed an extra junior accountant for a short period of time. The company went to a reputable agency and employed an appropriately qualified person. The company relied on the agency's screening policy which had failed to uncover a series of discrepancies in the accountant's personal history, including a false address. The accountant removed a company chequebook from his work place and used it to make a series of high value purchases on his own behalf. The matter came to light when a routine enquiry was made with the finance house to verify the issue of one of the cheques. By this time the temporary accountant had left the company. He could not be traced and the matter was referred to the police.

All in a week's work

In another case, an organisation employed a temporary accounts clerk to work in their shared service accounting centre. The organisation assumed the recruitment agency would perform adequate checks on the clerk's background. This did not happen. The clerk was able to use his access to the accounting system to divert supplier payments to his own bank account. After a week of such diversions, he left the company with over £150,000.

Reproduced with kind permission of the Fraud Advisory Panel from *Fighting fraud – a guide for SMEs,* 2nd edition

3.4 Summary

In conclusion, a sound ethical culture and an effective system of internal control are essential elements of an anti-fraud strategy. Effective internal controls reduce exposure to financial risks and 'contribute to the safeguarding of assets, including the prevention and detection of fraud' (Turnbull Guidance, 2005). However, a sound system of internal control cannot provide complete protection against all fraudulent behaviour, highlighting the importance of other fraud prevention and fraud detection measures.

Appendix 7 provides an example of a 16 step fraud prevention plan that brings together many of the elements described in this chapter.

4 Fraud detection

4.1 Detection methods

Hindsight is a wonderful thing! Fraud is always obvious to the fraudster's colleagues after the event. Their statements, and those of internal auditors, when taken by the police or other investigatory bodies, frequently highlight all the more common fraud indicators.

However, the mistake is always the same – fraud was never considered a possibility. No matter how innocent an action may be, or how plausible an explanation may be, fraud is always a possibility!

The UK report of PwC's survey looked at the method of detection of the most serious frauds within organisations. The results are shown in Figure 6.

It is clear from this, and other anecdotal evidence, that external auditors do not generally find fraud. As mentioned in Chapter 3, it is not the external auditor's responsibility to prevent and detect fraud, although they should be providing reasonable assurance that the financial statements are free from material fraud and error.

Figure 6 Methods of fraud detection

Source: *Economic crime: people, culture and controls,* PricewaterhouseCoopers, 2007

Although external auditors did not detect many cases of fraud, internal auditors on the other hand were found to be the most successful in identifying serious frauds. Risk management procedures were also found to be one of the more useful methods. If resources will allow it, an organisation should establish a strong internal audit function that monitors and advises on risk management and actively looks for instances of fraud.

Frauds may also be discovered as a result of controls and mechanisms put in place on the advice of internal and external auditors.

A lot of frauds, however, are discovered accidentally or as a result of information received, either via a tip off or through a whistleblowing hotline. In many cases, greater losses are suffered as a result of employees at all levels ignoring the obvious. It is everyone's responsibility to find and report fraud and irregularity within an organisation, and it is therefore essential that an organisation has appropriate reporting mechanisms in place to facilitate this.

Case study 7

Tipped off

A bank clerk who helped fraudsters to fleece customers out of nearly £500,000 was originally identified as a result of a tip off. Ruth Akinyemi passed on the personal details of eight wealthy Barclays account holders, including dates of birth and account passwords. The thieves to whom she gave the details then posed as real customers and emptied vast amounts of money from the bank accounts. One victim lost nearly £400,000 in just four days.

Investigators received an anonymous tip off that Akinyemi was the insider and she was suspended pending investigation. Due to insufficient supporting evidence, the bank initially cleared Akinyemi of any involvement. She simply switched branches and continued with the scam. The computer system revealed the involvement of a bank insider in subsequent frauds and investigators were able to go through computer records and identify the accounts that Akinyemi had accessed using her ID and password.

Akinyemi was convicted of conspiracy to steal and sentenced to 18 months imprisonment in September 2008. The operators of the fraud have never been traced and most of the money is still missing.

4.2 Indicators and warnings

It will never be possible to eliminate all fraud. No system is completely fraud proof, since many fraudsters are able to bypass control systems put in place to stop them. However, greater attention paid to some of the most common indicators can provide early warning that something is not quite right and increase the likelihood that the fraudster will be discovered. With that in mind, this section provides details of some of the more common indicators of fraud.

Fraud indicators fall into two categories:
- warning signs
- fraud alerts.

Warning signs
Warning signs have been described as organisational indicators of fraud risk and some examples are set out below. For convenience these have been subdivided into business risk, financial risk, environmental risk and IT and data risk. Further examples of warning signs can be found in Appendix 6.

Business risk
This has been subdivided into cultural issues, management issues, employee issues, process issues and transaction issues.

Cultural issues
- Absence of an anti-fraud policy and culture.
- Failure of management to implement a sound system of internal control and/or to demonstrate commitment to it at all times.

Management issues
- Lack of financial management expertise and professionalism in key accounting principles, review of judgements made in management reports and the review of significant cost estimates.
- A history of legal or regulatory violations within the organisation and/or claims alleging such violations.
- Strained relationships within the organisation between management and internal or external auditors.
- Lack of management supervision of staff.
- Lack of clear management control of responsibility, authorities, delegation, etc.
- Bonus schemes linked to ambitious targets or directly to financial results.

Employee issues
- Inadequate recruitment processes and absence of screening.
- Unusually close relationships – internal and external.
- Potential or actual labour force reductions or redundancies.
- Dissatisfied employees who have access to desirable assets.
- Unusual staff behaviour patterns.
- Personal financial pressures on key staff.
- Low salary levels of key staff.
- Poor dissemination of internal controls.
- Employees working unsocial hours unsupervised.
- Employees not taking annual leave requirements.
- Unwillingness to share duties.

Process issues
- Lack of job segregation and independent checking of key transactions.
- Lack of identification of the asset.
- Poor management accountability and reporting systems.
- Poor physical security of assets.
- Poor access controls to physical assets and IT security systems.
- Lack of and/or inadequacy of internal controls.
- Poor documentation of internal controls.

Transaction issues
- Poor documentary support for specific transactions such as rebates and credit notes.
- Large cash transactions.
- Susceptibility of assets to misappropriation.

Financial risk
- Management compensation highly dependent on meeting aggressive performance targets.
- Significant pressures on management to obtain additional finance.
- Extensive use of tax havens without clear business justification.
- Complex transactions.
- Use of complex financial products.
- Complex legal ownership and/or organisational structures.
- Rapid changes in profitability.
- Existence of personal or corporate guarantees.

Environmental risk
- The introduction of new accounting or other regulatory requirements, including health and safety or environmental legislation, which could significantly alter reported results.
- Highly competitive market conditions and decreasing profitability levels within the organisation.
- The organisation operating in a declining business sector and/or facing prospects of business failure.
- Rapid technological changes which may increase potential for product obsolescence.
- Significant changes in customer demand.

IT and data risk
- Unauthorised access to systems by employees or external attackers.
- The wealth of malicious codes and tools available to attackers.
- Rapid changes in information technology.
- Users not adopting good computer security practices, e.g. sharing or displaying passwords.
- Unauthorised electronic transfer of funds or other assets.
- Manipulation of programs or computer records to disguise the details of a transaction.
- Compromised business information.
- Breaches in data security and privacy.
- Sensitive data being stolen leaked or lost.

Fraud alerts

Fraud alerts have been described as specific events or red flags, which may be indicative of fraud. A list of possible fraud alerts is provided below. This should not be considered an exhaustive list, as alerts will appear in many different guises according to circumstances.

- Anonymous emails/letters/telephone calls.
- Emails sent at unusual times, with unnecessary attachments, or to unusual destinations.
- Discrepancy between earnings and lifestyle.
- Unusual, irrational, or inconsistent behaviour.
- Alteration of documents and records.
- Extensive use of correction fluid and unusual erasures.
- Photocopies of documents in place of originals.
- Rubber Stamp signatures instead of originals.
- Signature or handwriting discrepancies.
- Missing approvals or authorisation signatures.
- Transactions initiated without the appropriate authority.
- Unexplained fluctuations in stock account balances, inventory variances and turnover rates.
- Inventory adjustments.
- Subsidiary ledgers, which do not reconcile with control accounts.
- Extensive use of 'suspense' accounts.
- Inappropriate or unusual journal entries.
- Confirmation letters not returned.
- Supplies purchased in excess of need.
- Higher than average number of failed login attempts.
- Systems being accessed outside of normal work hours or from outside the normal work area.
- Controls or audit logs being switched off.

The above lists of fraud indicators can be indicative of any fraud type. Appendix 6 provides examples of more specific fraud indicators.

4.3 Tools and techniques

The training received by management accountants is a very good basis for implementing an anti-fraud programme. The broad understanding of business processes, expected of a management accountant, is an important asset, as is their knowledge of the systems and procedures that should be in place within an organisation, to allow it to operate efficiently and effectively. A further asset is the ability to think and act logically, which is something the management accountant develops with experience. Therefore, the first important tool available is training and experience.

The second tool is the necessary mindset – that fraud is always a possibility. A healthy amount of professional scepticism should be maintained when considering the potential for fraud. This does not mean that every time someone seems to be working excessive overtime, without taking leave, they are in the process of committing a fraud, or that inaccuracies in the accounts are there to cover up a fraud. Nevertheless, they might. Having considered the possibility of fraud, the next step may be to undertake some further research or pass concerns to a line manager.

In addition to the tools described above, there are everyday techniques available to help identify irregularities which may be fraud, and research the anomaly to decide whether further action should be taken. Organisations should ensure that resources are allocated to identifying such anomalies and detecting cases of fraud.

Identifying anomalies

Background reading: it is important to keep up to date with fraud trends and issues. The general press can be a useful source of information for this, along with technical magazines, which often carry articles on fraud and financial irregularity. Also useful is a subscription to a publication specialising in fraud or buying a good reference book. The Internet is also a valuable, and vast, research tool.

Risk assessment: undertake a fraud risk assessment and design specific tests to detect the significant potential frauds identified through the risk assessment. Act on irregularities which raise a concern.

Benchmarking: comparisons of one financial period with another; or the performance of one cost centre, or business unit, with another; or of overall business performance with industry standards, can all highlight anomalies worthy of further investigation.

Systems analysis: it is important to examine the systems in place and identify any weaknesses that could be opportunities for the fraudster.

Ratio analysis: can be used to identify any abnormal trends or patterns.

Mathematical modelling: using the 'sort' tool on a spreadsheet can help to identify patterns in expenditure, etc. There are also specialist mathematical models such as Benfords Law, a mathematical formula which can help identify irregularities in accounts. Database modelling can also be utilised.

Specialist software: such as audit tools for data matching analysis can prove very useful. Other tools allow for analysis such as real time transaction assessment, targeted post-transactional review, or strategic analysis of management accounts.

Exception reporting: many systems can generate automatic reports for results that fall outside of predetermined threshold values (exceptions), enabling immediate identification of results deviating from the norm. With today's technology it is possible for an email or text alert to be sent directly to a manager when exceptions are identified.

Many of these identification techniques can be automated to make the process more efficient. Fraud detection systems should be monitored and updated regularly to keep up with changing technology and new methods of manipulation.

Case study 8

Risk or returns

Many retail companies are investing in specialist fraud prevention and detection software and have quickly seen the benefits from doing so:

- Within weeks of implementing new data-mining software, clothing retailer Peacocks dismissed five employees for fraudulent activities identified by the fraud detection tool and a further 15 investigations were underway based on information highlighted by the software. Employee were found to be involved in activities such as processing genuine sales for customers then voiding the transaction, taking money from the tills, and applying refunds to their own credit cards. Peacocks believe that the increased chances of detection will stop some fraud before it is even committed. Peacocks are also using the system to pinpoint process improvement and training requirements.

- Boots saw its investment in loss-prevention software 'returned in only a matter of weeks' and have found that it continues to deliver reduced fraud losses that would have cost the business millions. The software sends an automatic message to store managers when anomalies in till transactions are identified, such as an above average number of refunds.

- In just over a year of using data-mining software, Lloydspharmacy identified around £400,000 of 'previously invisible fraud' and dismissed a number of 'unscrupulous employee(s). One of the main types of fraud suffered by Lloydspharmacy is where a till operator suspends a sale and then uses a 'no-sale' facility to open the till drawer. The linked activity between suspended sales and no sales can be easily identified using data-mining software though. The first investigation was within two weeks of the system going live and in the following year there were more than 100 investigations. The investigation payback increased through using data-mining software and further analysis showed that successful investigations have led to higher sales figures in the stores concerned. Introduction of the software has also freed loss prevention managers to focus on other activities, such as risk assessment and training.

- B&Q claims that its investment in a till monitoring system saved the company '£1 million on staff fraud in a year'.

Source: various articles from *Retail Week*

Analysing the anomaly – a methodical approach
All of the tools covered so far have their uses in identifying the irregularity, but to be effective they must be combined with a methodical approach to the analysis of the problem identified. At this stage, it is not a fraud investigation or internal management review but an analysis of a problem to decide whether such a review should be carried out. One approach which can be considered is detailed below.

1 Establish the objective
The objective of the research must be clear as this will enable decisions to be made about the best way forward.

2 Identify the systems and procedures
Undertaking a systems and risk analysis, and comparing the laid-down systems and procedures that should have been in place with those actually in use, can help to identify system or procedural failures.

3 Establish the scale of the risk
This involves identifying the potential loss and assessing whether it is material. Actual losses should be identified where possible.

4 Situation analysis
This involves background research, such as company searches, and identifying those involved.

5 Analyse all available data
Analysis of all the data will give an understanding of what has occurred and how it occurred.

6 Prepare schedules (include graphics)
Graphical and numerical schedules/spreadsheets should be prepared to support the analysis and findings. It is important to make it as easy as possible for those with little or no financial knowledge to understand what has occurred. These, when consolidated, would be in the form of an audit pack detailing the documents that have led to the formulation of the conclusions.

7 Prepare the report
In preparing the report it is important to bear in mind that, whatever the original objective, there is always the possibility of it being used in evidence at some form of legal proceedings. The report should be factual as far as possible, and where opinion is given, it should be clearly identified as such – for example, professional opinion used in the conclusions of the report.

4.4 Summary

Included in this chapter and in Appendix 6 are examples of specific fraud alerts associated with activities common to most types of organisation. However, none of these will be of any use unless it is accepted that fraud is possible. It is that mindset, that awareness, which will enable an organisation to stop an incidence of fraud before it becomes catastrophic. A warning sign is not effective unless it is appreciated as such and this awareness can only be achieved by means of a continuing programme of education and training.

5 Responding to fraud

An organisation's approach to dealing with fraud should be clearly described in its fraud policy and fraud response plan. An outline fraud response plan and an example of a fraud response plan are contained in Appendices 8 and 9 respectively. Appendix 9 includes a series of flowcharts that help to highlight the decisions an organisation might face when a fraud is suspected and give guidance on process to follow in response to such suspicions.

This chapter expands on parts of the outline fraud response plan, where they have not already been covered in earlier chapters, and highlights some issues and considerations when dealing with fraud. Paragraph headings in this chapter are those which should form the basis of the fraud response plan and relate to those in the outline response plan in Appendix 8.

5.1 Purpose of the fraud response plan

The fraud response plan is a formal means of setting down clearly the arrangements which are in place for dealing with detected or suspected cases of fraud. It is intended to provide procedures which allow for evidence gathering and collation in a manner which will facilitate informed decision-making, while ensuring that evidence gathered will be admissible in the event of any civil or criminal action. Other benefits arising from the publication of a corporate fraud response plan are its deterrence value and the likelihood that it will reduce the tendency to panic. It can help restrict damage and minimise losses, enable the organisation to retain market confidence, and help to ensure the integrity of evidence.

5.2 Corporate policy

The fraud response plan should reiterate the organisation's commitment to high legal, ethical and moral standards in all its activities and its approach to dealing with those who fail to meet those standards. It is important that all those working in the organisation are aware of the risk of fraud and other illegal acts, such as dishonesty or damage to property. Organisations should be clear about the means of enforcing the rules or controls which the organisation has in place to counter such risks and be aware of how to report any suspicions they may have. The fraud response plan is the means by which this information is relayed to all members of staff and, possibly, other stakeholders, such as customers, suppliers, and shareholders.

One question worthy of consideration is – how much publicity should be given to exposed fraud? A publicised successful fraud investigation can be a sharp reminder to those who may be tempted and a warning to those who are responsible for the management of controls. While there may be embarrassment for those who were close to the fraud and did not identify it, and an adverse impact on the organisation's public image, there can be advantages in publishing internally the outcome of a successful fraud investigation.

Regulated financial services companies do not have a choice on whether or not to keep identified cases of fraud an internal issue. These organisations are now legally obliged to report financial crime. Other businesses should follow this example and make it clear that they will not sweep fraud under the carpet.

Case study 9

Reporting fraud

It is possible to exaggerate the risks involved in reporting fraud. Aid to the Church in Need UK suffered a high tech website attack in November 2005 which led to hundreds of its benefactors being defrauded. 'The press were surprised by how we went public and that we admitted what had happened – but as a Christian charity we decided we had to be honest and we hope that others will learn from this case about the 'conspiracy of silence' over internet fraud. 98% of people have been very understanding.'

Reproduced with kind permission of the Fraud Advisory Panel from its Ninth Annual Review 2006-2007
Ethical behaviour is the best defence against fraud

5.3 Definition of fraud

As has been explained in Chapter 1, fraud encompasses criminal offences that involve deception and dishonesty to obtain some benefit or to cause detriment to some person or organisation. This section of a fraud response plan could provide for legal definitions or simply a list of activities which would or could be considered fraudulent.

5.4 Roles and responsibilities

The division of responsibilities for fraud risk management will vary from one organisation to the next, depending on the size, industry, culture and other factors. The following are some general guidelines which can be adapted to suit the individual circumstances.

Managers and supervisors
Generally managers and supervisors are in a position to take responsibility for detecting fraud and other irregularities in their area. Staff must assist management by reporting any suspected irregularities. Managers and supervisors should be provided with a response card, or aide-memoire, detailing how they should respond to a reported incidence of fraud. The aide-memoire should include a list of contacts with telephone numbers.

Finance director
The finance director will often have overall responsibility for the organisation's response to fraud, including the responsibility for co-ordinating any investigation and for keeping the fraud response plan up to date. They will hold the master copy of the fraud response plan, and should have their own aide-memoire to assist with the management of the investigation. The finance director will also be responsible for maintaining an investigation log. An investigations log is typically a log of all reported suspicions, including those dismissed as minor or otherwise not investigated. The log will contain details of actions taken and conclusions reached. It is an important tool for managing, reporting and evaluating lessons learned.

Fraud officer (where applicable)
In larger organisations it may be appropriate to designate a senior manager as the fraud officer in place of the finance director. The fraud officer will have responsibility for initiating and overseeing all fraud investigations, for implementing the fraud response plan and for any follow-up actions. The fraud officer should be authorised to receive enquiries from staff confidentially and anonymously, and be given the authority to act and/or provide advice according to individual circumstances, and without recourse to senior management for approval. In the event that the fraud officer's superior is a suspect, he should report to a more senior manager or non executive director, perhaps the chair of the audit committee.

The fraud officer will manage any internal investigations and act as a liaison officer with all other interested parties both internal and external, including police, regulators and auditors. He should have his own job description, appropriate to the role, an extended list of contacts and his own response card. One of his primary tasks would be the updating of the investigation log.

Human resources
The human resources department will usually have responsibility for any internal disciplinary procedures, which must be in line with, and support, the fraud policy statement and fraud response plan. Their advice should be sought in relation to the organisation's personnel management strategies, individual employment histories, and issues relating to employment law, or equal opportunities.

Audit committee (where applicable)
Due to recent legislative and regulatory changes (as set out in Chapter 1 and Appendix 1), the role of the audit committee in preventing and detecting fraud is now more defined. Audit committee members have responsibility for reviewing the organisation's internal control and risk management systems, including the design and implementation of anti-fraud programmes and controls. The audit committee should monitor the integrity of the financial statements, assess the organisation's performance in fraud prevention, review the investigation log of cases at least once a year, and report any significant matters to the board.

The audit committee should review arrangements by which employees can confidentially raise concerns about possible wrongdoing, and the audit committee's objective should be to ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up action. If a suspicion involves the nominated fraud contact, the finance director or an executive director, the matter should be reported directly to the chairman of the audit committee. In small companies a nominated non executive director may fulfil the role of the audit committee. The audit committee is also responsible for reviewing and evaluating the effectiveness of the internal audit function, where one exists.

Internal auditors (where applicable)
Where an organisation has its own internal audit department the likelihood is that the task of investigating any incidence of fraud would fall to them. Caution should be exercised in allowing an investigation to be conducted by those without training and experience in this area, as this may jeopardise the outcome of an investigation. It may be appropriate to designate specific auditors as fraud specialists and to ensure that they have the appropriate skills and knowledge to undertake the task.

External auditors (where applicable)
An organisation without its own internal audit department may consider consulting their external auditors should they discover a fraud, if only to obtain the expertise to establish the level of loss. The external auditors may also be in a position to provide expert assistance from elsewhere within the audit firm, such as from a specialist fraud investigation group. A decision to call on external auditors should, however, be considered carefully, as there is always the possibility that if the auditor has missed obvious fraud alerts, the organisation may eventually seek damages from its auditor.

Legal advisers (internal or external)
Legal advice should be sought as soon as a fraud is reported, irrespective of the route the organisation intends to follow. Specific advice would include such issues as guidance on civil, internal and criminal responses, and recovery of assets.

IS/IT staff
IS and IT staff can provide technical advice on IT security, capability and access. If computers have been utilised to commit the fraud, or if they are required for evidential purposes, specialist advice must be sought immediately.

Public relations (PR)
Organisations with a high profile, such as larger businesses, public sector organisations or charities, may wish to consider briefing their PR staff, so they can prepare a brief for the press in the event that news of a fraud becomes public.

Police
When the police are consulted, if at all, is a matter of internal policy in the UK. However, if it is policy to prosecute all those suspected of fraud, then the police should be involved at the outset of any investigation, as any unnecessary delay could diminish the likelihood of success. In respect of public bodies, Audit Commission guidance states that the police/external auditors should be informed as soon as a fraud is suspected.

External consultants
Any organisation could consider bringing in specialist investigation skills from outside the organisation. Many such specialist firms exist to provide a discreet investigation and/or asset recovery service in accordance with their clients' instructions.

Insurers
Many organisations take out fidelity insurance to protect themselves against large fraud losses. The timeframe for a report to fidelity insurers, and any additional requirements, should be included in the fraud response plan and is usually laid down in the insurance document.

5.5 The response

Reasonable steps for responding to detected or suspected instances of fraud include:
- clear reporting mechanisms
- a thorough investigation
- disciplining of the individuals responsible (internal, civil and/or criminal)
- recovery of stolen funds or property
- modification of the anti-fraud strategy to prevent similar behaviour in the future.

Reporting suspicions
The procedures for reporting fraud should be spelt out clearly and succinctly. This may be by means of a formal whistleblowing policy, as outlined in Chapter 3, but the procedures should also be summarised within the fraud response plan.

Establish an investigation team
After recording details of the allegations, the finance director, or the fraud officer if appropriate, should call together the investigation team and the organisation's advisers. This could involve any, or all, of those listed above.

Formulate a response
The objectives of the investigation should be clearly identified, as should the resources required, the scope of the investigation, and the timescale. The objectives of the investigating team will be driven by the organisation's attitude to fraud and the preferred outcome for dealing with fraud. An action plan should be prepared and roles and responsibilities should be delegated in accordance with the skills and experience of the individuals involved. The individual in overall control of the investigation should be clearly identified, as should the powers available to team members. Reporting procedures and procedures for handling and recording evidence should be clearly understood by all concerned.

Case study 10

TNT roots out fraud

The security function of TNT, a leading global express and mail business, conducts professional investigations into suspected cases of fraud and has embedded procedures for dealing with whistleblowers.

It has also taken the lead in developing proactive measures against fraud as a way of improving integrity for all stakeholders. TNT carries out security financial reviews of its business units aimed at identifying, analysing and dealing with the red flags of fraud.

Parallel with the security financial review, employers are trained through the TNT integrity programme, which was developed by a newly created group integrity department in conjunction with other key departments, including security and corporate audit.

Simon Scales, TNT's Deputy Global Security and Compliance Director, says: 'Prevention is better than cure. It's about doing the right things as well as doing things right.'

Source: *Cut out a rotten core, Excellence in Leadership,* Issue 2 2007

5.6 The investigation

Preservation of evidence
A key consideration in any investigation must always be how to secure or preserve sufficient evidence to prove a case of fraud. It is vitally important that control is taken of any physical evidence before the opportunity arises for it to be removed or destroyed by the suspect(s). Physical evidence may therefore need to be seized at an early stage in the investigation, before any witness statements are collected or interviews conducted. If a criminal act is suspected, the police should also be consulted early in the process, before any overt action is taken and the suspect is alerted.

In English and Welsh law, for the purposes of criminal proceedings, the admissibility of evidence is governed by the Police and Criminal Evidence Act 1984 (PACE). In addition, the Criminal Procedures and Investigations Act 1996 provides a statutory framework and code of practice for disclosure of material collected during the course of investigations. Although PACE does not apply in civil or disciplinary proceedings, it should nevertheless be regarded as best practice.

If an individual does end up being charged with a criminal offence, and this may not be planned at the outset of the investigation, all investigations, and relevant evidence arising from such investigations, will be open to discovery by that individual's defence. It is, therefore, important that proper records are kept from the outset, including accurate notes of when, where and from whom the evidence was obtained and by whom. The police, or legal advisers, will be able to advise on how this should be done.

If appropriate, written consent should be obtained from the relevant department or branch manager before any items are removed. This can be done with senior management authority, as the items are the organisation's own property. Similarly, electronic evidence must be secured before it can be tampered with by the suspect.

Physical evidence
If an internal investigation is being conducted, then an organisation has a right to access its own records and may bring disciplinary action against any member of staff who tries to prevent this. Where physical evidence is owned or held by other organisations or individuals who are not employees, it may be necessary to obtain a court order or injunction to secure access to or to allow seizure of the evidence. The exact means of obtaining physical evidence depends on the particular circumstances of the case and whether criminal or civil action is being pursued, or both.

When taking control of any physical evidence, original material is essential. Photocopies are not acceptable. Records should be kept of when it was obtained and the place that it was taken from. If evidence consists of several items, for example many documents, each one should be tagged with a reference number that corresponds with the written record. Taking photographs or video recordings of the scene, such as the suspect's office, may also prove helpful.

Electronic evidence
In order to ensure case integrity and compliance with current UK legislation, retrieval of electronic evidence should be treated in a similar manner to that of other physical evidence, although there will be some distinct differences. These are covered in the UK Good Practice Guide issued by the ACPO, which sets outs four principles for dealing with computer-based electronic evidence. These principles are as follows:

Principle 1
No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may be relied upon in court.

Principle 2
In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person MUST be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3
An audit trial or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4
The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Interviews (general)
Managers are quite entitled to interview staff under their direction and to ask them to account for assets which were, or are, under their direct control, or to explain their performance in respect of the management or supervision of specific employees. However, the point at which it is considered that there are reasonable grounds for suspicion of an individual is the point where questioning should be stopped and the individual advised that their actions will be the subject of a formal investigation (should criminal prosecution be considered). From this moment on any interviews should be conducted by trained personnel or by police officers. Detailed notes should be kept of questions and answers, and interviews should be taped if possible.

Statements from witnesses
If a witness is prepared to give a written statement, it is good practice for someone else, normally a trained or experienced manager, to take a chronological record of events using the witness's own words. The witness must be happy to sign the resulting document as a true record. The involvement of an independent person usually helps to confine the statements to the relevant facts and the witness should be given the opportunity to be supported by a colleague, acquaintance or trade union official.

Statements from suspects
If a criminal act is suspected, the requirements of PACE, and other legislation, must be considered before any interview with a suspect takes place, since compliance determines whether evidence is admissible in criminal proceedings. Before initiating any interview under caution, the interviewer must ensure that they fully understand the requirements of PACE, as laid down in the codes of practice issued in accordance with Section 66 of the Act. These codes are periodically reviewed and the most recent amendment to the codes came into effect from 1 February 2008. As PACE is essentially aimed at police officers and other trained investigators, if the need for an interview under caution arises, police involvement should again be considered.

The codes of practice under PACE do still apply to others, with Section 67 of the Act making it clear that 'Persons other than police officers who are charged with the duty of investigating offences, shall ...have regard to any relevant provision of such a code.' Failure to observe the codes of practice may therefore jeopardise vital evidence, rendering it useless. In practice, therefore, it is suggested that interviews should only be conducted by trained personnel, with advice and guidance from the organisations legal advisers or the police. This guidance could be supported by means of a brief or an aide-memoire for the personnel concerned and supplemented with formal training.

When conducting investigations it is also important to be mindful of the provisions of the Human Rights Act, in particular the rights to privacy and to a fair trial or hearing.

5.7 Organisation's objectives with respect to dealing with fraud

The thoroughness of an investigation may depend on the course of action that the organisation plans to take with regard to a case of fraud. The organisation's policy may include any or all of the following preferred outcomes in dealing with fraud.

Internal disciplinary action
In accordance with the organisation's personnel and disciplinary guidelines.

A civil response
Whereby action is taken through the civil courts to recover losses.

Criminal prosecution
Whereby action is taken against the individual(s) concerned in a police managed enquiry.

A parallel response
Where civil action to recover misappropriated assets is taken in parallel with a police investigation.

5.8 Follow-up action

Lessons learned
There are lessons to be learned from every identified incident of fraud, and the organisation's willingness to learn from experience is as important as any other response. The larger organisation may consider establishing a special group to examine the circumstances and conditions which allowed the fraud to occur, with a view to making a report to senior management detailing improvements to systems and procedures. A smaller organisation may consider discussing the issues with some of its more experienced people, with the same objectives in mind.

Management response
Internal reviews
Having experienced an incident of fraud, the organisation may consider a fundamental review of all of its systems and procedures so as to identify any other potential system failures or areas of weakness. Changes to systems or policy should be implemented as soon as possible.

Implement changes
Should weaknesses have been identified, it can only be of benefit to the organisation to take the appropriate remedial action. Recent statistics have again confirmed that many organisations suffer more than one incident of fraud per year.

Annual report
An investigations log should be maintained and an annual report should be submitted to the board of all investigations carried out, outcomes and lessons learned.

Enforcement policies
A growing number of organisations are introducing enforcement policies that highlight the organisation's zero tolerance approach to fraud and clearly state that if a case of fraud is identified, appropriate action will be taken and those responsible will be made an example of, no matter who the perpetrator is. For example, financial institutions are keen to demonstrate a commitment to dealing with wrongdoers and are increasingly prosecuting fraudulent employees rather than 'sweeping the matter under the carpet'.

5.9 Summary

It is important that organisations have a documented plan for responding to suspected or detected cases of fraud. A fraud response plan should include a clear statement on the corporate policy with regard to dealing with fraud, and set out the roles and responsibilities of those involved in responding to suspicions. It should outline how an investigation should be handled, ensuring that due process is followed and integrity of evidence is maintained. The fraud response plan may also detail follow up action that will be taken by an organisation in light of established incidents of fraud.

Appendix 1 Fraud and the law

UK law

The Fraud Act
The Fraud Act made fraud a criminal offence and provides for the following ways of committing the offence:

- fraud by false representation
- fraud by failing to disclose information
- fraud by abuse of position.

For each of the different ways of perpetrating fraud set out in the Fraud Act, the common theme is that a person has acted dishonestly with the intent to make a gain for himself or another, cause loss to another, or expose another to a risk of loss.

In addition to those listed above, the Fraud Act also covers the offences of carrying on a business fraudulently; making, supplying or possessing articles for use in frauds; and obtaining services dishonestly. These offences include the creation or possession of software which has been created or adapted for fraudulent use. The newly created fraud offences carry a maximum penalty of 10 years' imprisonment, a fine or both.

The Fraud Act affects both companies and individuals and is part of a wider initiative to combat the increasing problem of fraud. It has been loosely drafted so that it will be able to capture forms of fraud using the internet and new technologies. Previous legislation proved inadequate at keeping up with rapid developments in technology and the wide range of possible fraudulent activity resulting from it.

The Fraud Act also extends the territorial scope of previous legislation. Not all activities of the offence must take place in the UK in order for a prosecution under the Fraud Act. UK courts have jurisdiction even where the only activity to have taken place in the UK is the gain or loss of property.

The Companies Act 2006
The Companies Act in the UK has been subject to major reform, resulting in the Companies Act 2006, which came into force in its entirety in October 2008. The new legislation sets out a statutory statement of the general duties of directors and introduces a right for shareholders to sue directors individually for breach of these duties, either as a result of negligence or fraud.

The duties include:

- duty to promote the success of the company
- duty to exercise reasonable care, skill and diligence
- duty to avoid conflicts of interest
- duty to declare interests in proposed transactions or arrangements
- duty not to accept benefits from third parties.

The Companies Act 2006 includes the offence of fraudulent trading and also creates a new offence in relation to documents to be delivered to Companies House. Under Section 1112 of the Act, where a person knowingly or recklessly delivers or causes to be delivered a document or statement that is misleading, false or deceptive in a material particular, they will be liable to up to two years imprisonment, a fine, or both.

Public Interest Disclosure Act (PIDA)
PIDA is known as the whistleblowing law in the UK, as it offers protection to employees who blow the whistle in one of the ways set out in the Act. Under PIDA, employers should not victimise a 'worker' if they make 'qualifying disclosures'. PIDA's definition of a worker covers all forms of employment but excludes Crown Servants whose work covers national security issues, police officers and employees who ordinarily work outside the UK. Qualifying disclosures are defined as information which, in the reasonable belief of the worker making the disclosure, tends to show one or more of the following is either happening now, has happened already or is likely to happen:

- a criminal offence
- failure to comply with a legal obligation
- a miscarriage of justice
- danger to the health and safety of an individual
- damage to the environment
- deliberate concealment of information tending to show any of the above.

PIDA has a stepped disclosure regime, which helps to balance the public interest and the interests of employers. Under this regime, the worker will be protected if the disclosure is made to their employer, some other responsible person if the disclosure is relevant to that person, or to a third party, where this is in accordance with outlined and agreed procedures. PIDA most readily protects workers where disclosures are made internally.

With regard to internal disclosures, the worker is protected if the disclosure has been made in good faith and with reasonable belief that there has been wrongdoing. There are then different levels of external disclosure. Protection is given for disclosures to prescribed regulators where the worker reasonably believes that the information or allegation is substantially true. Wider public disclosures (including to the media or a consumer group) may still be protected under PIDA, and more readily so where whistleblowing arrangements are not in place within the organisation or are ineffective. There must be justifiable cause for going wider and the particular disclosure must be reasonable.

Serious Crimes Act
The Serious Crimes Act aims to improve the ability of law enforcement agencies to tackle fraud and other serious organised crime, and strengthen the recovery of criminal assets. It also introduces additional measures to prevent or disrupt serious crime, including the prevention of fraud. Most of the provisions of the Serious Crimes Act came into force in early 2008 and make several radical changes to criminal law.

The Serious Crimes Act gives certain courts in the UK the ability to issue serious crime prevention orders. These create a new form of civil injunction, the breach of which is a criminal act punishable by imprisonment and a fine. A prevention order can be imposed where the court is satisfied that a person (including an individual, a partnership or a company) has been involved in a serious crime and where it has reasonable grounds to believe the order would protect the public by prohibiting or restricting the person's activities, including financial holdings, business dealings, working arrangements and communications. Serious crimes covered by this Act include attempting, committing, facilitating or encouraging serious offences such as fraud, money laundering, corruption and bribery.

With regard to additional measures, the Serious Crimes Act makes new provisions for disclosure and information sharing by public authorities to any anti-fraud organisation, in order to prevent fraud or in relation to proceeds of crime. The government is to prepare a code of practice with respect to such disclosure. The Act also authorises certain bodies to conduct data matching exercises for the purpose of preventing or detecting fraud. This provision puts a statutory basis around the National Fraud Initiative that has operated in the UK for some years.

Proceeds of Crime Act (POCA)
POCA was brought into effect during 2002 and 2003, and allows for the civil recovery of the proceeds of crime. It consolidated existing laws on confiscation and money laundering into a single piece of legislation, in order to improve the efficiency of the recovery process and increase the amount of illegally obtained assets recovered from criminals.

POCA also created new money laundering offences and provided financial investigation officers with new investigative powers. Under POCA, a money laundering offence is committed where someone conceals, disguises, converts or transfers criminal property or removes it from the UK or even between countries with in the UK. It is also an offence to enter into an arrangement that one knows or suspects facilitates the acquisition, retention, use or control of criminal property. As such, partaking or assisting in many activities aimed at defrauding a business may also be money laundering offences.

Under POCA, there is no de minimis limit (i.e. it covers proceeds of any criminal conduct and not just 'serious' crime) and there is no requirement for the activities resulting in the offence to have been conducted in the UK. The Serious Organised Crimes and Police Act 2005 made some adjustments to POCA, intended to clarify the situation in cases where doubt arose under POCA.

The Asset Recovery Agency (ARA) was established under POCA in 2003. ARA had the powers to use civil court procedures to recover the proceeds of crime by way of an action in the High Court. However, from April 2008, ARA ceased to exist following its transfer to the Serious Organised Crime Agency under the provisions of the Serious Crimes Act.

For further information on money laundering, please refer to the Anti-Money Laundering page on CIMA's website (www.cimaglobal.com).

The Fraud Review
Between 2005 and 2006, the UK Attorney General's office conducted an extensive review of the national arrangements for dealing with fraud (The Fraud Review), with the aim of reducing the extent of fraud and minimising the harm that it causes to the economy and wider society.

The Fraud Review was completed in July 2006 with the publication of an extensive report that contained a number of recommendations covering measurement, reporting, prevention, investigation and prosecution of fraud. The report was welcomed by the government and selected key recommendations were taken forward as part of an integrated strategy to tackle fraud (the National Fraud Programme).

The National Fraud Programme includes:
- formation of a National Fraud Strategic Authority to co-ordinate strategy between organisations both in the public and private sectors who tackle fraud
- creation of a Fraud Loss Measurement Unit to provide robust estimates for the measurement of fraud losses and assessment of value and risks of future fraud threats
- enhanced data sharing provisions through creation of a National Fraud Reporting Centre and Intelligence Bureau
- creation of a National Lead Force for Fraud based on the City of London Police Fraud Squad to act as a centre of excellence
- extension of sentencing provisions through new powers for the Crown Court.

The National Fraud Programme brings a greater emphasis on prevention and deterrence of fraud, but spans the entire spectrum of counter fraud activity, including detection, prosecution, sanctioning, and redress for victims. In October 2007 the government announced that £29 million of new funding would be put forward to implement the National Fraud Programme and many of the recommendations have started to be put into place during 2008.

US law

Sarbanes-Oxley Act (Sarbox)
Sarbox is a US federal law. However, it is far reaching legislation and impacts on many businesses in the UK and globally, and has therefore been included in this guide. Sarbox was passed in US Congress in January 2002 and came into effect in November 2004. Compliance is mandatory for all companies listed in the US, regardless of the size of the company or where the company is actually based.

Sarbox was introduced in response to a number of major corporate and accounting scandals, the most well known probably being the collapses of Enron and WorldCom. The Act introduced major changes to the regulation of financial practice and corporate governance, aimed at improving accuracy and transparency around financial reporting and increasing oversight of the assurance process. Sarbox is a large piece of legislation, arranged into 11 titles. This guide will focus on the specific requirements relating to fraud risk management.

Sarbox targets the perceived drivers of financial statement fraud (or accounting fraud) by attempting to strengthen risk management and internal controls, increase board and audit committee oversight, improve auditor vigilance and independence, and create accounting fraud penalties that act as a significant deterrence. It requires companies to implement extensive corporate governance policies, procedures and tools to prevent and respond to fraudulent activity within the company.

Title 3 requires chief executives and chief financial officers (the signing officers) to certify the integrity of the financial reports. Pursuant to Section 302, the signing officers must attest that they have evaluated the internal control system and must give information on any fraud, regardless of materiality, that involves management or employees who have significant involvement in internal control activities.

Title 4 describes enhanced reporting requirements for financial transactions and includes Section 404. Section 404 of Sarbox is one of the more controversial parts of the act, and requires management and the external auditor to report on the effectiveness of the company's internal controls over financial reporting. The Securities Exchange Commission (SEC) has noted in its final rules for Section 404 that an adequate internal control structure must include 'controls related to the prevention, identification and detection of fraud.' This covers more than just accounting fraud. Insider trading, intellectual property theft, misappropriation of customer data and other internal frauds would all need to be considered. There has been debate over whether Sarbox, and Section 404 in particular, has been too onerous. In 2007, the SEC responded to this criticism by issuing management guidance to ensure that companies focus efforts on what truly matters. According to the Financial Reporting Council, the SEC has also identified the Turnbull guidance as a suitable framework for complying with the requirements of Section 404.

Title 8 describes specific penalties for altering, manipulating or destroying financial records or evidence in an investigation, and for defrauding shareholders of publicly traded companies. It is also referred to as the Corporate and Criminal Fraud Accountability Act of 2002, based on a fraud bill that was originally proposed following the fall out of Enron. Penalties include imprisonment of up to 20 years and fines of up to $5 million. Title 8 also includes protections for whistleblowers under Section 806. Procedures for handling whisteblower reports are covered by Section 301.

Title 9 increases the criminal penalties for white collar crimes and conspiracies, and is also called the White Collar Crime Penalty Enhancement Act of 2002. It recommends stronger sentencing guidelines and creates a new criminal offence of failure to certify corporate financial reports. Attempts and conspiracies to commit a criminal fraud offence are subject to the same penalties as committing the offence itself. Again, penalties of up to 20 years and fines of up to $5 million can be imposed.

Title 11 makes it a criminal offence to tamper with records and interfere with official proceedings, and is also known as the Corporate Fraud Accountability Act of 2002. It revises sentencing guidelines and strengthens the associated penalties. Under this title, the SEC has authority to temporarily freeze large or unusual payments to directors, officers, agents and employees of a company during investigations of security law violations. It also codifies the SEC's right to prohibit persons convicted of securities fraud from serving as a director or officer of a public company.

Sarbox also encourages companies to establish an ethical culture and requires disclosure of whether the company has adopted a code of ethics for senior finance officers. It also has whistleblower provisions to help uncover lapses in ethics and fraudulent behaviour.

Appendix 2 Examples of common types of internal fraud

This appendix looks at common types of internal fraud and some of the methods through which they may be perpetrated.

Asset misappropriation

Cash

Theft of cash
- Stealing from petty cash.
- Taking money from the till.
- Skimming of cash before recording revenues or receivables (understating sales or receivables).
- Stealing incoming cash or cheques through an account set up to look like a bona fide payee.

False payment requests
- Employee creating false payment instruction with forged signatures and submitting it for processing.
- False email payment request together with hard copy printout with forged approval signature.
- Taking advantage of the lack of time which typically occurs during book closing to get false invoices approved and paid.

Cheque fraud
- Theft of company cheques.
- Duplicating or counterfeiting of company cheques.
- Tampering with company cheques (payee/amount).
- Depositing a cheque into a third party account without authority.
- Cheque kiting (a fraud scheme using two deposit accounts to withdraw money illegally from the bank).
- Paying a cheque to the company knowing that insufficient funds are in the account to cover it.

Billing schemes
- Over-billing customers.
- Recording of false credits, rebates or refunds to customers.
- Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund).
- Using fictitious suppliers or shell companies for false billing.

Misuse of accounts
- Wire transfer fraud (fraudulent transfers into bank accounts).
- Unrecorded sales or receivables.
- Employee account fraud (where an employee is also a customer and the employee makes unauthorised adjustments to their accounts).
- Writing false credit note to customers with details of an employee's personal bank account or of an account of a company controlled by the employee.
- Stealing passwords to payment systems and inputting series of payments to own account.

Non-cash

Inventory and fixed assets
- Theft of inventory.
- False write offs and other debits to inventory.
- False sales of inventory.
- Theft of fixed assets, including computers and other IT related assets.
- Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans, etc).
- Receiving free or below market value goods and services from suppliers.
- Unauthorised private use of company property.
- Employees trading for their own account.

Procurement
- Altering legitimate purchase orders.
- Falsifying documents to obtain authorisation for payment.
- Forging signatures on payment authorisations.
- Submitting for payment false invoices from fictitious or actual suppliers.
- Improper changes to supplier payment terms or other supplier details.
- Intercepting payments to suppliers.
- Sending fictitious or duplicate invoices to suppliers.
- Improper use of company credit cards.
- Marked up invoices from contracts awarded to supplier associated with an employee.
- Sale of critical bid information, contract details or other sensitive information.

Payroll
- Fictitious (or ghost) employees on the payroll.
- Falsifying work hours to achieve fraudulent overtime payments.
- Abuse of commission schemes.
- Improper changes in salary levels.
- Abuse of holiday leave or time off entitlements.
- Submitting inflated or false expense claims.
- Adding private expenses to legitimate expense claims.
- Applying for multiple reimbursements of the same expenses.
- False workers' compensation claims.
- Theft of employee contributions to benefit plans.

Fraudulent statements

Financial

Improper revenue recognition
- Holding the books open after the end of the accounting period.
- Inflation of sales figures which are credited out after the year end.
- Backdating agreements.
- Recording fictitious sales and shipping.
- Improper classification of revenues.
- Inappropriate estimates for returns, price adjustments and other concessions.
- Manipulation of rebates.
- Recognising revenue on disputed claims against customers.
- Recognising income on products shipped for trial or evaluation purposes.
- Improper recording of consignment or contingency sales.
- Over/under estimating percentage of work completed on long-term contracts.
- Incorrect inclusion of related party receivables
- Side letter agreements (agreements made outside of formal contracts).
- Round tripping (practice whereby two companies buy and sell the same amount of a commodity at the same price at the same time. The trading lacks economic substance and results in overstated revenues).
- Bill and hold transactions (where the seller bills the customer for goods but does not ship the product until a later date).
- Early delivery of product/services (e.g. partial shipments, soft sales, contracts with multiple deliverables, up front fees).
- Channel stuffing or trade loading (where a company inflates its sales figures by forcing more products through a distribution channel than the channel is capable of selling).

Misstatement of assets, liabilities and/or expenses
- Fictitious fixed assets.
- Overstating assets acquired through merger and acquisitions.
- Improper capitalisation of expenses as fixed assets (software development, research and development, start up costs, interest costs, advertising costs).
- Manipulation of fixed asset valuations.
- Schemes involving inappropriate depreciation or amortisation.
- Incorrect values attached to goodwill or other intangibles.
- Fictitious investments.
- Improper investment valuation (misclassification of investments, recording unrealised investments, declines in fair market value/overvaluation).
- Fictitious bank accounts.
- Inflating inventory quantity through inclusion of fictitious inventory.
- Improper valuation of inventory.
- Fraudulent or improper capitalisation of inventory.
- Manipulation of inventory counts.
- Accounts receivable schemes (e.g. creating fictitious receivables or artificially inflating the value of receivables).
- Misstatement of prepayments and accruals.
- Understating loans and payables.
- Fraudulent management estimates for provisions, reserves, foreign currency translation, impairment, etc.
- Off balance sheet items.
- Delaying the recording of expenses to the next accounting period.

Other accounting misstatements

- Improper treatment of inter-company accounts.
- Non clearance or improper clearance of suspense accounts.
- Misrepresentation of suspense accounts for fraudulent activity.
- Improper accounting for mergers, acquisitions, disposals and joint ventures.
- Manipulation of assumptions used for determining fair value of share based payments.
- Improper or inadequate disclosures.
- Fictitious general ledger accounts.
- Journal entry fraud (using accounting journal entries to fraudulently adjust financial statements).
- Concealment of losses.

Non-financial

- Falsified employment credentials e.g. qualifications and references.
- Other fraudulent internal or external documents.

Corruption

Conflicts of interest

Kickbacks

- Kickbacks to employees by a supplier in return for the supplier receiving favourable treatment.
- Kickbacks to senior management in relation to the acquisition of a new business or disposal of part of the business.
- Employee sells company-owned property at less than market value to receive a kickback or to sell the property back to the company at a higher price in the future.
- Purchase of property at higher than market value in exchange for a kickback.
- Preferential treatment of customers in return for a kickback.

Personal interests

- Collusion with customers and/or suppliers.
- Favouring a supplier in which the employee has a financial interest.
- Employee setting up and using own consultancy for personal gain (conflicts with the company's interests).
- Employee hiring someone close to them over another more qualified applicant.
- Transfer of knowledge to a competitor by an employee who intends to joins the competitor's company.
- Misrepresentation by insiders with regard to a corporate merger, acquisition or investment.
- Insider trading (using business information not released to the public to gain profits from trading in the financial markets).

Bribery and extortion

Bribery

- Payment of agency/facilitation fees (or bribes) in order to secure a contract.
- Authorising orders to a particular supplier in return for bribes.
- Giving and accepting payments to favour or not favour other commercial transactions or relationships.
- Payments to government officials to obtain a benefit (e.g. customs officials, tax inspectors).
- Anti-trust activities such as price fixing or bid rigging.
- Illegal political contributions.

Extortion

- Extortion (offering to keep someone from harm in exchange for money or other consideration).
- Blackmail (offering to keep information confidential in return for money or other consideration).

Appendix 3 Example of a risk analysis

The risk analysis set out below is an example of the results of an assessment by a risk management group of the fraud risks in the contracts function. This document is a summary of the work undertaken by the risk management group, and they will have working papers to document their workings and assessments.

The risks identified are in the first column, and the dates of the risk assessment in the second column. The column Probability/likelihood records the assessment of the likelihood of this risk occurring in the organisation. The ratings are graded high, medium or low. The next column, impact, is an assessment of the impact of a fraud in this area. The next column records the assessment of the controls in this area, and the net likely impact is an assessment of the likelihood of a fraud not being detected by the controls. At this stage the risks in the contracts area can be reviewed and priorities set for action to address the risk.

Take for example, the risks relating to an unchanging list of suppliers. The risk management group believes fraud has a high likelihood of occurring and if so, it could cause significant financial loss to the business. The controls are thought to be weak and unlikely to reduce the risk. They have assessed the net likely impact to be high and recommend that this is an immediate priority in the contracts area.

Factor/risk area and description contracts	**Date of assessment**	**Probability/ likelihood**	**Impact**	**Controls impact**	**Net likely**	**Action**
Unchanging list of preferred suppliers	2007	High	High	Low	High	Priority – immediate
Consistent list of single source suppliers	2007	Medium	High	High	Medium	–
Changes in contract specifications	2007	Low	Low	Medium	Low	–
Personal relationships between staff and suppliers	2008	Low	High	Low	High	Priority – within x months

Appendix 4 A sample fraud policy

The following is an example of a policy which can be modified for use by any organisation.

Background

This organisation has a commitment to high legal, ethical and moral standards. All members of staff are expected to share this commitment. This policy is established to facilitate the development of procedures which will aid in the investigation of fraud and related offences.

The board already has procedures in place that reduce the likelihood of fraud occurring. These include standing orders, documented procedures and documented systems of internal control and risk assessment. In addition the board tries to ensure that a risk and fraud awareness culture exists in this organisation.

This document, together with the fraud response plan and investigator's guide, is intended to provide direction and help to those officers and directors who find themselves having to deal with suspected cases of theft, fraud or corruption. These documents give a framework for a response and advice and information on various aspects and implications of an investigation. These documents are not intended to provide direction on prevention of fraud.

Fraud policy

This policy applies to any irregularity, or suspected irregularity, involving employees as well as consultants, suppliers, contractors, and/or any other parties with a business relationship with this organisation. Any investigative activity required will be conducted without regard to any person's relationship to this organisation, position or length of service.

Actions constituting fraud

Fraud comprises both the use of deception to obtain an unjust or illegal financial advantage and intentional misrepresentations affecting the financial statements by one or more individuals among management, staff or third parties.

All managers and supervisors have a duty to familiarise themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert for any indications of irregularity.

The board's policy

The board is absolutely committed to maintaining an honest, open and well intentioned atmosphere within the organisation. It is, therefore, also committed to the elimination of any fraud within the organisation, and to the rigorous investigation of any such cases.

The board wishes to encourage anyone having reasonable suspicions of fraud to report them. Therefore, it is also the board's policy, which will be rigorously enforced, that no employee will suffer in any way as a result of reporting reasonably held suspicions.

All members of staff can therefore be confident that they will not suffer in any way as a result of reporting reasonably held suspicions of fraud. For these purposes 'reasonably held suspicions' shall mean any suspicions other than those which are shown to be raised maliciously and found to be groundless. The organisation will deal with all occurrences in accordance with the Public Interest Disclosure Act.

Appendix 5 Sample whistleblowing policy

Introduction

This whistleblowing policy has been introduced in response to the Public Interest Disclosure Act 1998 and provides a procedure which enables employees to raise concerns about what is happening at work, particularly where those concerns relate to unlawful conduct, financial malpractice or dangers to the public or the environment. The object of this policy is to ensure that concerns are raised and dealt with at an early stage and in an appropriate manner.

This organisation is committed to its whistleblowing policy. If an employee raises a genuine concern under this policy, he or she will not be at risk of losing their job, nor will they suffer any form of detriment as a result. As long as the employee is acting in good faith and in accordance with this policy, it does not matter if they are mistaken.

How the whistleblowing policy differs from the grievance procedure

This policy does not apply to raising grievances about an employee's personal situation. These types of concern are covered by the organisation's grievance procedure. The whistleblowing policy is primarily concerned with where the interests of others or of this organisation itself are at risk. It may be difficult to decide whether a particular concern should be raised under the whistleblowing policy or under the grievance procedure or under both. If an employee has any doubt as to the correct route to follow, this organisation encourages the concern to be raised under this policy and will decide how the concern should be dealt with.

Protecting the employee

This organisation will not tolerate harassment or victimisation of anyone raising a genuine concern under the whistleblowing policy. If an employee requests that their identity be protected, all possible steps will be taken to prevent the employee's identity becoming known. If the situation arises where it is not possible to resolve the concern without revealing the employee's identity (e.g. if the employee's evidence is needed in court), the best way to proceed with the matter will be discussed with the employee. Employees should be aware that by reporting matters anonymously, it will be more difficult for the organisation to investigate them, to protect the employee and to give the employee feedback. Accordingly, while the organisation will consider anonymous reports, this policy does not cover matters raised anonymously.

How the matter will be handled

Once an employee has informed the organisation of his or her concern, the concerns will be examined and the organisation will assess what action should be taken. This may involve an internal enquiry or a more formal investigation. The employee will be told who is handling the matter, how they can contact him/her and whether any further assistance may be needed. If the employee has any personal interest in the matter, this should be declared by the employee at the outset. If the employee's concern falls more properly within the grievance procedure, then they will be advised of this.

How to raise a concern internally

Step 1
If an employee has a concern about malpractice, he or she should consider raising it initially with their line manager. This may be done orally or in writing. An employee should specify from the outset if they wish the matter to be treated in confidence so that appropriate arrangements can be made.

Alternatively, employees can call the 24 hour whistleblowing telephone hotline. This service is strictly confidential and callers will not be asked to give their name if they do not want to.

Step 2
If these channels have been followed and the employee still has concerns, or an employee feels that they are unable to raise a particular matter with their line manager, for whatever reason, they should raise the matter with their head of department, the head of human resources or the chief internal auditor.

Independent advice

If an employee is unsure whether to use this procedure or wants independent advice at any stage, they may contact the independent charity Public Concern at Work on 020 7404 6609. Their lawyers can give free confidential advice at any stage about how to raise a concern about serious malpractice at work. An employee can, of course, also seek advice from a lawyer of their own choice at their own expense.

External contacts

It is intended that this policy should give employees the reassurance they need to raise concerns internally. However, this organisation recognises that there may be circumstances where employees should properly report matters to outside bodies, such as regulators or the police. If an employee is unsure as to whether this is appropriate and does not feel able to discuss the matter internally, Public Concern at Work will be able to give advice on such an option and on the circumstances in which an employee should contact an outside body rather than raise the matter internally.

Matters raised maliciously

Employees who are found to maliciously raise a matter that they know to be untrue will be subject to the disciplinary policy.

Appendix 6 Examples of fraud indicators, risks and controls

The following are examples of indicators for two specific types of fraud – procurement fraud and fraud in the selling process. There are many other types of fraud and each will have its own set of indicators as well as some of the general indicators that are set out in Chapter 4.

Example 1: Procurement fraud

Fraud in the purchasing or procurement function is a particular risk. The following may be indicators of fraud in the tendering and contract award process.

Before contract award
- Disqualification of suitable tenderers.
- 'Short' invitation to tender list.
- Unchanging list of preferred suppliers.
- Consistent use of single source contracts.
- Contracts specifications that do not make commercial sense.
- Contracts that include special, but unnecessary specifications, that only one supplier can meet.
- Personal relationships between staff and suppliers.

During the contract award process
- Withdrawal of a lower bidder without apparent reason and their subsequent sub-contracting to a higher bidder.
- Flexible evaluation criteria.
- Acceptance of late bids.
- Changes in the specification after bids have been opened.
- Consistently accurate estimates of tender costs.
- Poor documentation of the contract award process.
- Consistent favouring of one firm over others.

After the award of contract
- Unexplained changes in the contract after its award.
- Contract awarded to a supplier with a poor performance record.
- Split contracts to circumvent controls or contract conditions.
- Suppliers who are awarded contracts disproportionate to their size.
- Frequent increases in the limits of liability.
- Frequent increases in contract specifications.

Organisations may wish to consider at invitation to tender acknowledgement stage, or at bid submission, formally requesting the tenderer to sign a document confirming that no fraud or corrupt practice has occurred when developing the bid.

This has two effects:

1 It acts as a deterrent – tenderers are alerted to the fact that the client is aware of the risk of fraud and will be on the lookout for any evidence that it has occurred.

2 It ensures that should something fraudulent come to light, tenderers can have no excuse that they were unaware of the client's policy.

Activity	Fraud risk	Prevention
Scoping of contract	The contract specification is written in a manner which favours a particular technical, end user and financial supplier.	Use of control/assessment panel made up of representatives, to ensure that more than one person is involved in drawing up the specification.
Contract documentation	Conditions of contract are changed to accommodate a favoured supplier, or , to exclude competitors	Standard contract conditions and specifications to be used. Any variations to be approved by senior management.
Setting evaluation criteria	Original evaluation criteria are changed after the receipt of submissions to ensure that favoured suppliers are shortlisted	Use evaluation criteria as agreed by the contract panel prior to tendering. Where EU procurement rules apply evaluation criteria are required to be stated in advance.
Contractual correspondence	Altering terms and conditions to suit a preferred supplier	Contract terms and conditions should be those of the purchasing department and not subject to change without the written approval of senior management.
Contact management	False claims for work not carried out, or exaggerated claims for actual work done	Clear audit trails with written records. Authorisation of changes to original documentation. Random and systematic checks of activity.
Claims negotiation	Assisting the contactor to justify claims.	Claims negotiation should be carried out using professional advisers.
Certification	Inadequate certification may lead to overpayments, or payments for work not carried out.	Clear separation of duties between ordering the work, certification and authorisation for payment. Certification documents should be returned to the originator.
Authorisation	Contract splitting to keep contract values under a particular staff member's authorisation financial limit.	The splitting of contacts should not be allowed unless authorised by senior management. Internal controls should be established to detect this.
Pricing	Tender prices appear to drop whenever a new supplier is invited to bid.	Management reviews of the reasonableness and competitiveness of prices
Suppliers	Contract awarded to a company with a poor performance record.	Ensure contractors with a poor performance record are removed from the approved supplier's list.
	Contract awarded to a contractor who is not the lowest tenderer.	Senior management review.

Tender procedure – audit checks
Tender board: Should be chaired by senior manager.

Tender register: Should be held and reviewed by a senior manager.

Checks should include:
- Were all tenders secured in a locked cabinet/box prior to opening?
- Who had access to the keys/combination?
- If no tender box/cabinet utilised, what is the procedure for dealing with tenders?
- Does the tender register show an unbroken, sequentially numbered and dated list of all tenders received?
- Were all the entries signed by the tender board chairperson?
- Confirm that tender lists show no evidence of patronage or incestuous relationships.
- Confirm that firms which persistently fail to tender are excluded from subsequent tender lists.
- Has relevant approval been obtained before accepting any tenders whose prices exceed approval limits?
- Has relevant approval been obtained where the lowest compliant bid is not accepted?
- In the event of a clear differential in bid prices confirm that the same tender specification has been sent to all prospective tenderers.
- Confirm that there is no excessive use of single sources of supply or tender action.
- Confirm that the tender board has been advised of the signs which would indicate tender rigging/ringing.
- Confirm that the recommended method of procurement has been followed.
- Confirm that the contract makes commercial sense.

Example 2: Fraud in the selling process

Fraud risks also exist in the selling process. Those involved can include any combination of the clients' management or staff and the organisation's own management or staff, with or without any collusion.

The following are indicators of fraud in the selling process:
- Overcharging from an approved list or standard profit mark-up.
- Short-changing by not delivering the contracted quantity or quality.
- Diversion of orders to a competitor or associate.
- Bribery of a customer by one of the organisation's own sales representatives.
- Bribery of a customer by a competitor – no proper explanation of why the contract went elsewhere.
- Insider information by knowing competitor's prices.
- False warranty claims that are made or paid.
- Over selling of goods or services that are not necessary.
- Giving of free issues/samples when not necessary
- Links with cartels or 'rings'.
- Bribery to obtain contracts which would not otherwise be awarded.
- Issuing invoices or credit notes which do not reflect reality and of which the ultimate payer is unaware.
- Issuing credit notes to hide additional discounts or rebates.
- The use of sales intermediaries (fixers).
- Sales commission gates, which can often cause misreporting of orders.

Appendix 7 A 16 step fraud prevention plan

1. Consider fraud risk as an integral part of your overall corporate risk-management strategy.
2. Develop an integrated strategy for fraud prevention and control.
3. Develop an ownership structure from the top to the bottom of the organisation.
4. Introduce a fraud policy statement.
5. Introduce an ethics policy statement.
6. Actively promote these policies through the organisation.
7. Establish a control environment.
8. Establish sound operational control procedures.
9. Introduce a fraud education, training and awareness programme.
10. Introduce a fraud response plan as an integral part of the organisation's contingency plans.
11. Introduce a whistle-blowing policy.
12. Introduce a reporting hotline.
13. Constantly review all anti-fraud policies and procedures.
14. Constantly monitor adherence to controls and procedures.
15. Establish a learn from experience group.
16. Develop appropriate information and communication systems.

Source: *Defence Mechanism, Financial Management,* September 2002

Appendix 8 Outline fraud response plan

1 Purpose of the fraud response plan

2 Corporate policy

3 Definition of fraud

4 Roles and responsibilities
- Managers and supervisors
- Finance director
- Fraud officer
- Human resources
- Audit committee
- Internal auditors
- External auditors
- Legal advisers
- IS/IT staff
- Public relations
- The police
- External consultants
- Insurers

5 The response
- Reporting suspicions
- Establish an investigation team
  - objectives
  - reporting procedures
  - responsibilities
  - powers
  - control
- Formulate a response
  - in accordance with corporate policy

6 The investigation
- Preservation of evidence
- Physical evidence
- Electronic evidence
- Interviews (general)
- Statements from witnesses
- Statements from suspects

7 Organisation's objectives with respect to fraud
- Internal report
  - no further action
  - disciplinary action
- Civil response
  - legal advisers' control
  - legal submissions
  - case file
- Criminal response
  - police controlled
  - case file
- Parallel response
  - civil recovery
  - criminal prosecution

8 Follow up action
- Lessons learned
- Management response
  - internal reviews
  - implement changes
  - annual report
  - enforcement policies

Appendix 9 Example of a fraud response plan

This example has been based on a response plan from an organisation within the UK's NHS.

1 Introduction

This document is intended to provide direction and help to those officers and directors who find themselves having to deal with suspected cases of theft, fraud or corruption. It gives a framework for a response and provides information on various aspects of investigation. The document also contains a series of flowcharts which provide a framework of procedures that allow evidence to be gathered and collated in a way which facilitates informed initial decisions, while ensuring that evidence gathered will be admissible in any future criminal or civil actions. This document is not intended to provide direction on fraud prevention.

2 Corporate policy

The board is committed to maintaining an honest, open and well intentioned atmosphere within the organisation. It is, therefore, also committed to the elimination of all fraud and to the rigorous investigation of any such cases.

The board wishes to encourage anyone who has reasonable suspicions of fraud to report them. The organisation has a published whistleblowing policy which aims to ensure that concerns are raised and dealt with in an appropriate manner. Employees raising genuine concerns will be protected and their concerns looked into.

3 The definitions of fraud

The term fraud encompasses a number of criminal offences involving the use of deception to obtain benefit or causing detriment to individuals or organisations.

This document is intended to provide a framework for investigating all suspected cases of fraud, theft or corruption where:

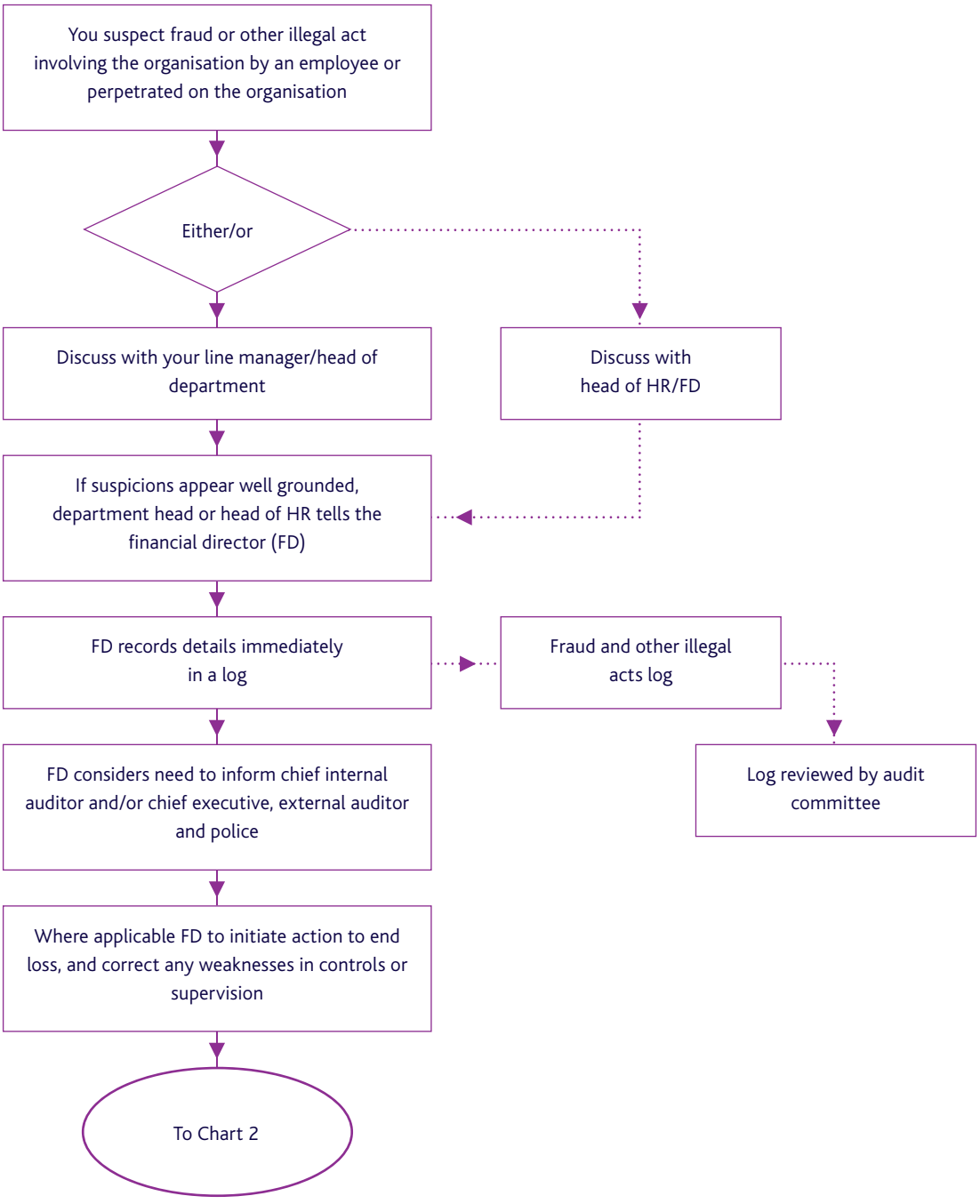
- the value of the organisation has suffered or may have suffered; or
- has been misrepresented for personal gain

as a result of the actions or omissions of:

- directors and staff employed by the organisation; or
- customers, contractors and other external stakeholders.

4 Roles and responsibilities

Chart 1 Reporting fraud



Finance director
Responsibility for investigating fraud has been delegated to the finance director. Where appropriate/ necessary he is also responsible for informing third parties such as the external auditors or the police about the investigations. The finance director will inform and consult with the chief executive in cases where the loss is potentially significant or where the incident may lead to adverse publicity.

The finance director will maintain a log of all reported suspicions, including those dismissed as minor or otherwise not investigated. The log will contain details of actions taken and conclusions reached and will be presented to the audit committee for inspection annually.

The finance director will normally inform the chief internal auditor at the first opportunity. While the finance director will retain overall responsibility, responsibility for leading any investigation will be delegated to the chief internal auditor. Significant matters will be reported to the board as soon as practical.

Chief internal auditor
The chief internal auditor will:
- initiate a diary of events to record the progress of the investigation throughout
- agree the objectives, scope and timescale of the investigation and resources required with the finance director at the outset of the investigation;
- ensure that proper records of each investiation are kept from the outset, including accurate notes of when, where and from whom evidence was obtained and by whom.

Head of human resources
Where a member of staff is to be interviewed or disciplined the finance director and/or chief internal auditor will consult with, and take advice from, the head of human resources.

The head of human resources will advise those involved in the investigation in matters of employment law, company policy and other procedural matters (such as disciplinary or complaints procedures) as necessary.

Line and other managers
If, in accordance with the organisation's whistleblowing policy, a member of staff raises a concern with their line manager, head of department or the head of human resources the details must be immediately passed to the finance director for investigation. If a concern involves the finance director, the matter should be reported directly to the audit committee.

Staff
All staff have a responsibility to protect the assets of the organisation, including information and goodwill as well as property.

5 Objectives with respect to fraud

See Chart 2 – managing the investigation

Investigations will try to establish at an early stage whether it appears that a criminal act has taken place. This will shape the way that the investigation is handled and determine the likely outcome and course of action.

If it appears that a criminal act has not taken place, an internal investigation will be undertaken to:

- determine the facts
- consider what, if any, action should be taken against those involved
- consider what may be done to recover any loss incurred
- identify any system weakness and look at how internal controls could be improved to prevent a recurrence.

The chief internal auditor will present the findings of his investigation to the finance director who will make the necessary decisions and maintain a record of the subsequent actions in relation to closing the case. Once concluded, details of such cases will be reported to the audit committee on an annual basis for information.

Where an investigation involves a member of staff and it is determined that no criminal act has taken place the finance director will liaise with the head of human resources and appropriate line manager to determine which of the following has occurred and therefore whether, under the circumstances, disciplinary action is appropriate:

- gross misconduct (i.e. acting dishonestly but without criminal intent)
- negligence or error of judgement was seen to be exercised
- nothing untoward occurred and therefore there is no case to answer.

The disciplinary procedures of the organisation will be followed in any disciplinary action taken towards an employee. This will usually involve a disciplinary hearing at which the results of the investigation will be considered.

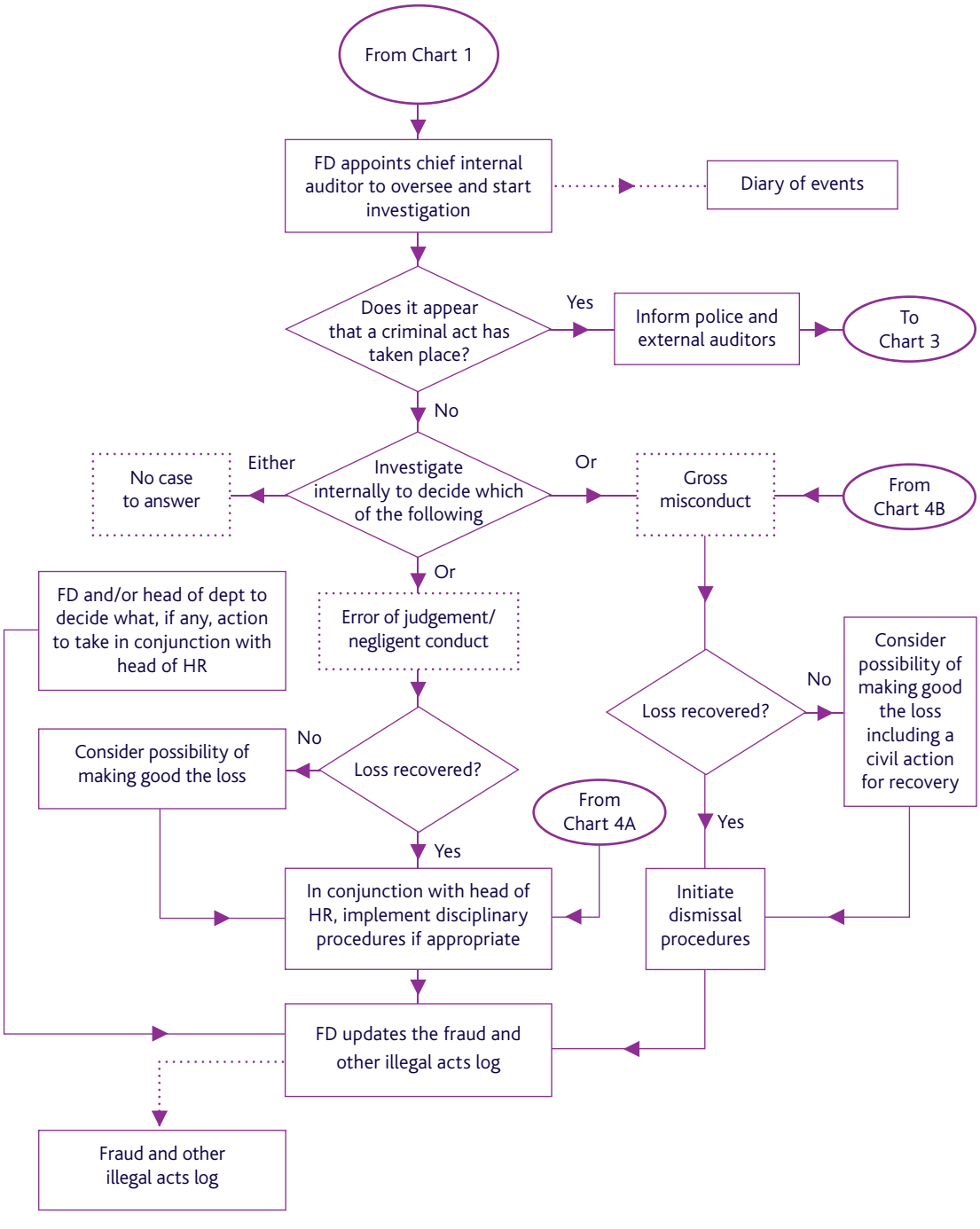
Where, after having sought legal advice, the finance director judges it cost effective to do so, the organisation will normally pursue civil action in order to recover any losses. The finance director will refer the case to the organisation's legal advisers for action.

Where initial investigations point to the likelihood of a criminal act having taken place the chief internal auditor will, with the agreement of the finance director, contact the police and the organisation's legal advisers at once. The advice of the police will be followed in taking forward the investigation.

Where there are sufficient grounds, the organisation will, in addition to seeking recovery of losses through civil proceedings, also seek a criminal prosecution. The finance director will be guided by the police in arriving at his decision on whether a criminal prosecution is to be pursued.

Where appropriate the finance director will consider the possibility of recovering losses from the organisation's insurers.

Chart 2 Managing the investigation



6 The response

See Charts 3 and 4 – gathering evidence and interview procedure.

The chief internal auditor will normally be responsible for managing investigations, including interviewing witnesses and gathering any necessary evidence. However, each case will be treated according to the particular circumstances and professional advice will be sought where necessary. Where there are reasonable grounds for suspicion, the police will be involved at an early stage but the chief internal auditor may still undertake part or all of the investigations on their behalf, as agreed between the finance director, chief internal auditor and the police.

Witness statements
If a witness is prepared to give a written statement the head of HR or chief internal auditor will take a chronological record using the witness's own words. The witness will be asked to sign the document as a true record.

Physical and electronic evidence
The chief internal auditor will take control of any physical evidence and maintain a record of where, when and from whom it was taken. Where the evidence consists of several items these will be tagged with a reference number which corresponds with the written record of the investigation. He should also ensure that electronic evidence is appropriately handled.

Before interviewing any suspect(s) the chief internal auditor will provide a verbal or written report of the investigation to the finance director. The finance director may consult others e.g. head of human resources, the chief executive and the police before reaching a decision on how to proceed.

Interviewing suspect(s)
If the finance director decides to proceed with interviewing a suspect, and where the suspect is an employee of the organisation, the interview will usually be carried out by the line manager and head of human resources. The individual(s) being interviewed should be informed of the reason for the interview and a contemporaneous record will be made of all that is said. They should also be advised that they are not under arrest and are free to leave at any time. The individual(s) being interviewed will also be given the opportunity to be supported by a friend or trade union official. This type of interview will not take place under caution. If the need for caution arises during the course of an interview, the interview will be terminated immediately after the caution is given and the individual concerned advised to seek legal advice. The finance director will be notified and police advice sought at this point. Once the interview is over, the suspect will be given the opportunity to read the written record and sign each page in acknowledgement of its accuracy. All other persons present will also be asked to sign to acknowledge accuracy.

Where external organisations/individuals are involved, interviews will generally be undertaken by the police unless the finance director is able to gain the co-operation of the organisation's management or auditors.

Chart 3 Gathering evidence

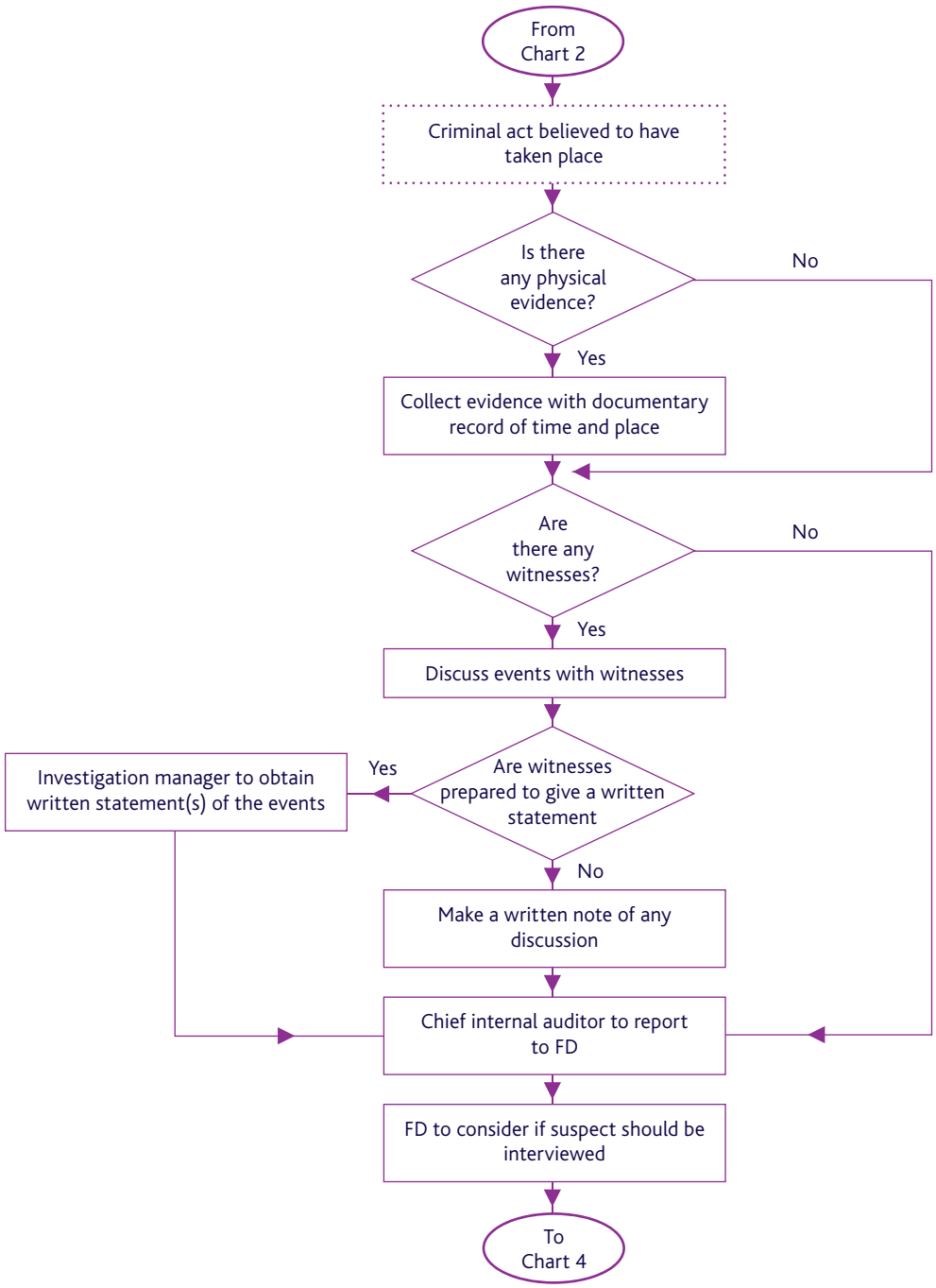
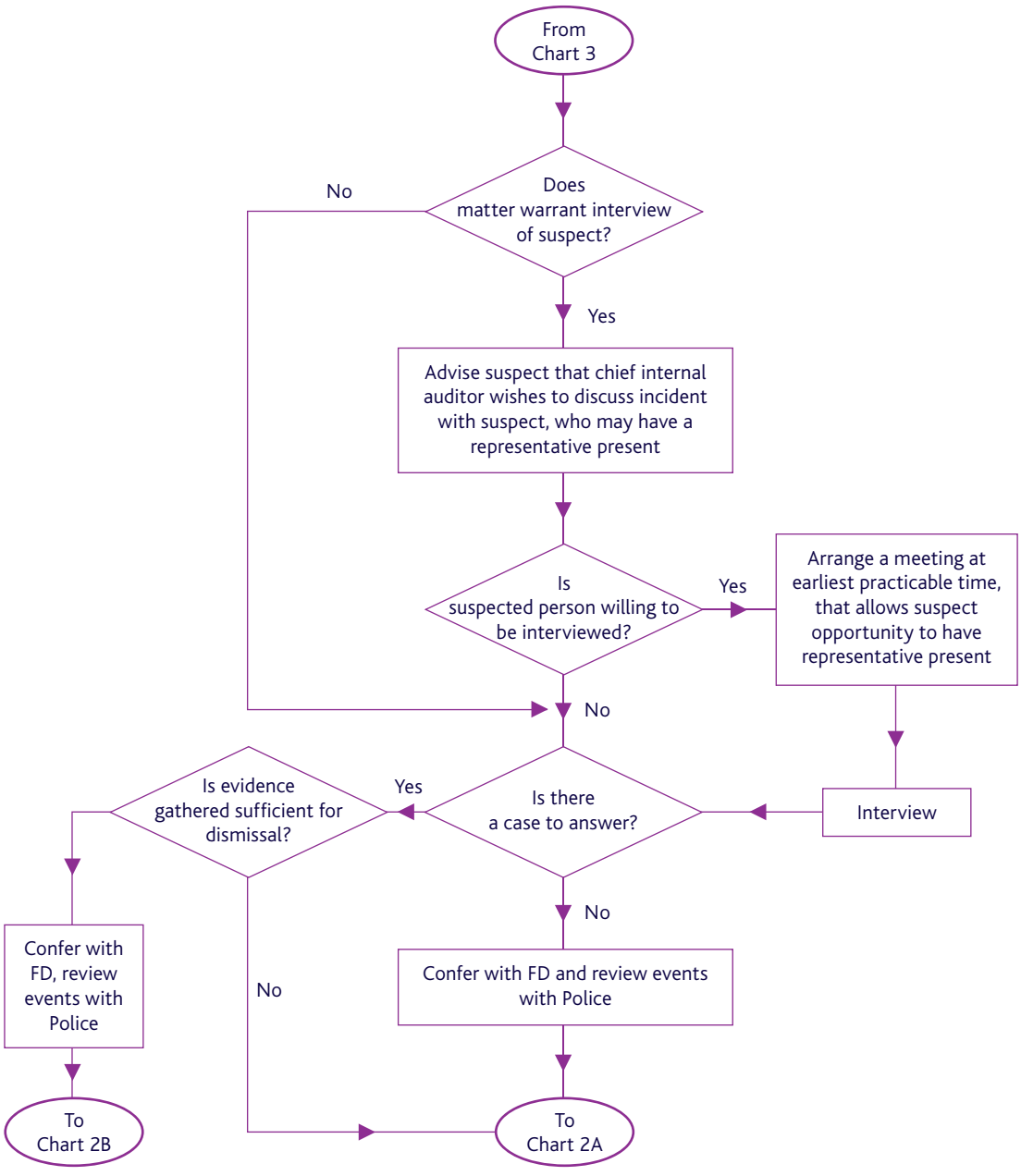


Chart 4 Interview procedure



Appendix 10 References and further reading

The Association of certified fraud examiners (ACFE), (2008), *Report to the Nation on Occupational Fraud and Abuse,* **www.acfe.org**

The Association of certified fraud examiners, ACFE, (2008), *Fraud Examiners Manual.*

BDO Stoy Hayward LLP, (January 2008), BDO *Fraudtrack 5: A global challenge,* **www.bdo.co.uk/fraudtrack**

BT Group (2008), *BT The way we work: a statement of business practice,* **www.bt.com**

BSi British Standards, (2008), *Whistleblowing Arrangements Code of Practice, PAS 1998-2008,* **www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/Risk/PAS-19982008-Whistleblowing**

CIMA (2000), *Corporate Governance – History, Practice and Future.*

CIMA, (2005), *CIMA Official Terminology.*

CIMA, (2002), *Risk Management: A guide to good practice.*

CIMA and the IBE, (2008), *Managing responsible business.*

Collier, P.M. and Agyei-Ampomah, S., (2007), *CIMA Official Learning System Management Accounting Risk and Control Strategy.*

DirectNews, (2007), *Weak anti-fraud measures earn bank hefty fine,* CIMA Industry Focus.

Ernst & Young, (2003), *Fraud, the Unmanaged Risk,* **www.ey.com**

FEE Brussels, (2005), *How SME's can reduce the risk of fraud,* **www.fee.be/publications**

Felson, M. and Clarke, R., (1999), *Opportunity Makes the Thief, Police Research Series 98,* London: Home Office.

Finn, J. and Cafferty, D., (September 2002), *Defence Mechanism,* Financial Management.

Fisher, C. and Lovell, A., (2000), *Accountants Responses to Ethical Issues at Work.*

Fraud Advisory Panel, (2006), *Sample Fraud Policy Statements,* **www.fraudadvisorypanel.org**

Fraud Advisory Panel, (2006), *Fighting Fraud: A guide for SME's 2nd Edition.*

Fraud Advisory Panel, (2006-2007), *Ninth Annual Review 2006-2007 Ethical behaviour is the best defence against fraud.*

HM Treasury, (May 2003), *Managing the Risk of Fraud.*

Institute of Business Ethics, (2003), *Developing a Code of Business Ethics: A guide to best practice including the IBE Illustrative Code of Business Ethics.*

Institute of Business Ethics, (2007), *Does Business Ethics Pay?*

Institute of Business Ethics, *Good Practice Guide, Speak up Procedures* **www.ibe.org.uk/SpeakUp**

Institute of Business Ethics, *Living Up to our values: developing ethical assurance,* **www.ibe.org.uk/LUTOVcontents_overview.pdf**

The Institute of internal auditors, The Association of certified public accountants, The Association of certified public examiners, (2008), *Managing the business risk of fraud: A practical guide.*

International Federation of Accountants (IFAC), (2006), *International Auditing and Assurance Standards Board, ISA's 240,300,315 and 330.*

Iyer, N. and Samociuk, M., (2006), *Fraud and Corruption: Prevention and Detection.*

Iyer, N. and Samociuk, M., (2007), *Rotten to the Core,* Excellence in Leadership Issue 2, SPG Media.

Kroll and the Economist Intelligence Unit, (2007/2008), *Kroll Global Fraud Report, Annual Edition 2007/2008,* **www.kroll.com/about/library/fraud**

Kroll and the Economist Intelligence Unit, (2008/2009), *Kroll Global Fraud Report Annual Edition 2008/2009,* **www.kroll.com/about/library/fraud**

KPMG, (2007), *Profile of a Fraudster Survey 2007,* **www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey**

Levi, M., Burrows J., Flemming, M.H., and Hopkins, M., with the assistance of Matthews, K., (2007), *The Nature, extent and economic impact of fraud in the UK.*

PricewaterhouseCoopers, (2007), *Economic Crime: people, culture and controls The 4th biennial Global Economic Crime Survey United Kingdom,* **www.pwc.com/crimesurvey**

PricewaterhouseCoopers, (2007), *Economic Crime: people, culture and controls The 4th biennial Global Economic Crime Survey,* **www.pwc.com/crimesurvey**

Professional Accountants in Business committee, (2006), *Defining and developing an effective code of conduct.*

Turner, C., (2007), *Fraud risk management: a practical guide for accountants.*

Wells, J., (2007), *Corporate fraud handbook: prevention and detection 2nd ed.* Hoboken, NJ: John Wiley and Sons.

Useful Web links

Governance

Combined Code on Corporate Governance **www.frc.org.uk/corporate/combinedcode.cfm**

European Corporate Governance Network: **www.ecgn.org**

Good governance standard for public services, CIPFA, **www.opm.co.uk/index.html**

How to use Turnbull to comply with Sarbox **www.frc.org.uk/documents/pagemanager/frc/draft_guide.pdf**

International Corporate Governance Network: **www.icgn.org**

OECD Anti-Corruption Unit: **www.oecd.org/daf/nocorruptionweb**

Legislation

Companies Act 2006 **www.opsi.gov.uk/ACTS**

Fraud Act in 2006 **www.opsi.gov.uk/ACTS**

Police and Criminal Evidence Act 1984 (PACE), **www.police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro**

Proceeds of Crime Act 2002 **www.opsi.gov.uk/acts**

Public Interest Disclosures Act (PIDA) **www.opsi.gov.uk/acts**

Sarbanes – Oxley Act 2002 (Sarbox) **www.soxlaw.com**

Serious Crimes Act 2007 **www.opsi.gov.uk/ACTS**

Organisations

Financial Services Authority (FSA): **www.fsa.gov.uk**

Fraud Advisory Panel: **www.fraudadvisorypanel.org**

ISACA: **www.isaca.org**

National Fraud Strategic Authority:
www.attorneygeneral.gov.uk/national_fraud_strategic_authority_page.html

Public Concern at Work: **www.pcaw.co.uk**

Serious Fraud Office: **www.sfo.gov.uk**

Serious Organised Crime Agency (SOCA):
www.soca.gov.uk

World Bank Anti-Corruption Resource Center:
www1.worldbank.org/publicsector/anticorrupt

Appendix 11 Listed abbreviations

ACFE	Association of Certified Fraud Examiners
ACPO	Association of Chief Police Officers
ARA	Asset Recovery Agency
BDO	BDO Stoy Hayward LLP
BSi	British Standards Institute
CEE	Central & Eastern Europe
CEO	Chief executive officer
CIMA	The Chartered Institute of Management Accounts
CV	Curriculum vitae
EIU	Economist Intelligence Unit
FSA	Financial Services Authority
IBE	Institute of Business Ethics
IFAC	International Federation of Accountants
IP	Intellectual property
IS	Information securities
ISA	International Standard on Auditing
IT	Information technology
OECD	Organisation for Economic Co-operation and Development
PACE	Police and Criminal Evidence Act 1984
PAIB	Professional Accountants in Business
PAS	Publicly Available Specification
PIDA	Public Interest Disclosure Act 1998
POCA	Proceeds of Crime Act 2002
PR	Public relations
PwC's	PricewaterhouseCoopers
Sarbox	Sarbanes-Oxley Act 2002
SAS	Statement on Auditing Standards
SEC	Securities & Exchange Commission
SOCA	Serious Organised Crime Agency

978-1-85971-611-3 (pdf)

January 2009

Chartered Institute of
Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom

T. +44 (0)20 8849 2275
F. +44 (0)20 8849 2468
E. innovation.development@cimaglobal.com
www.cimaglobal.com

TEC050V0110