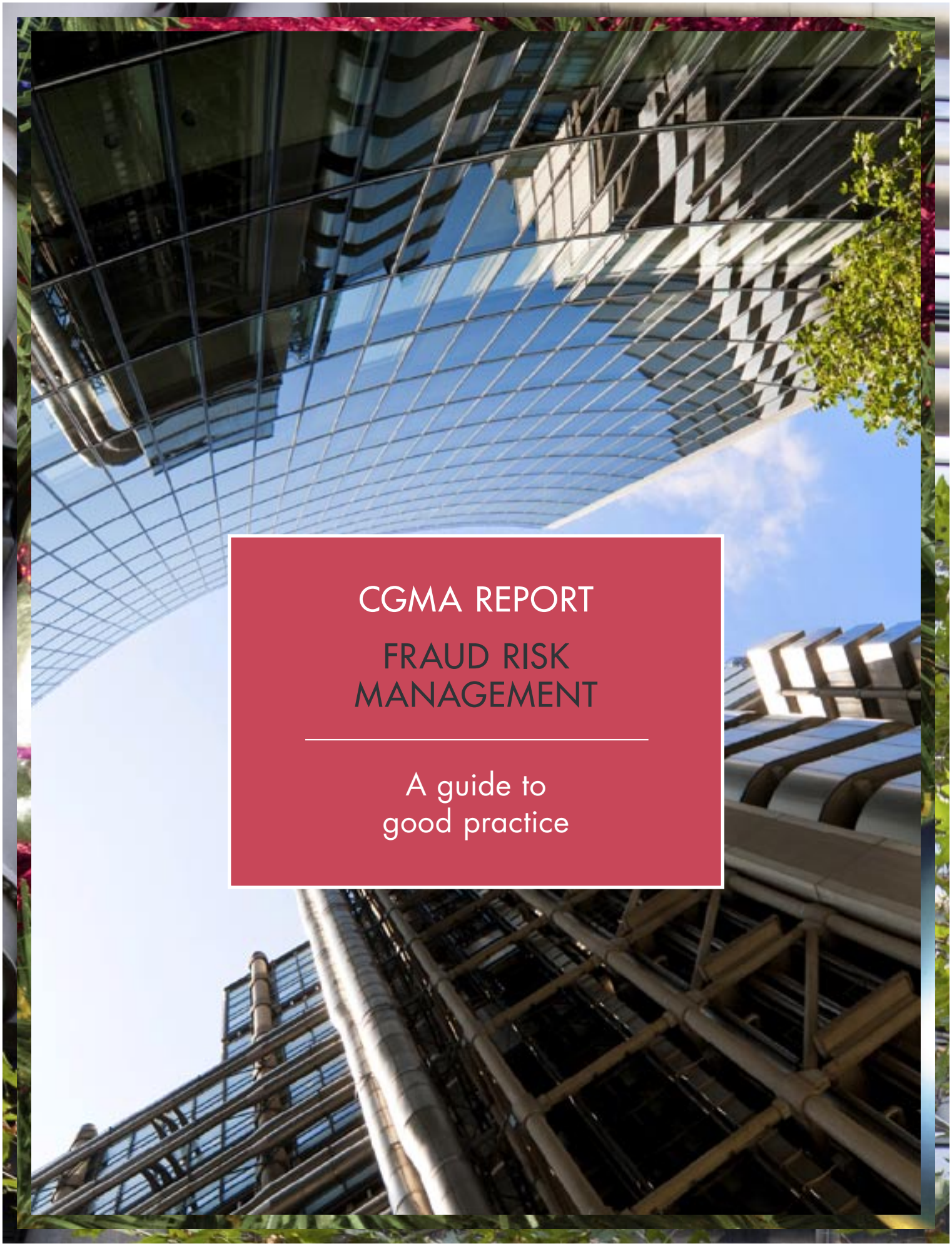


CGMA REPORT

FRAUD RISK MANAGEMENT

A guide to good practice

CGMA
Chartered Global Management Accountant

Powered by
AICPA | CIMA

CONTENTS

Two of the world's most prestigious accounting bodies, AICPA and CIMA, have formed a joint-venture to establish the Chartered Global Management Accountant (CGMA) designation to elevate the profession of management accounting. The designation recognises the most talented and committed management accountants with the discipline and skill to drive strong business performance.

Author
Gillian Lees is Head of Corporate Governance at CIMA

EXECUTIVE SUMMARY

1. Fraud is prevalent within organisations and remains a serious and costly problem for virtually every type of organisation in every part of the world. 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.

2. 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. Yet, most research shows that organisations which actively manage their fraud risk reap benefits in terms of reducing the negative impact of fraud.

3. While the law relating to fraud varies from country to country, there are **universal principles of fraud risk management** relating to prevention, detection and response. These can be applied by organisations of all sizes in any sector and/or country.

4. There is no universal definition of fraud. But it essentially involves using deception to make a personal gain dishonestly for oneself and/or create a loss for another.

5. There are **three key types of fraud** that affect organisations: asset misappropriation, fraudulent statements and corruption.

6. The fraud triangle is a useful model for understanding the motivation to commit fraud. It is built on the premise that fraud is likely to result from a combination of three factors: **motivation, opportunity and rationalisation.** An effective way of tackling fraud is to adopt methods that will address these factors.

7. An **effective anti-fraud strategy** has four main components:

   a. Prevention

   b. Detection

   c. Response

   d. Deterrence

   It is the combination of effective fraud prevention, detection and response measures that create an effective fraud deterrent.

8. Key components of a **fraud prevention strategy**:

   a. a sound ethical culture

   b. sound internal control systems.

9. A significant number of frauds are detected either accidentally or as a result of tip-offs. This reinforces the importance of **raising general fraud awareness** in the organisation and emphasising that it is everyone's responsibility in the organisation to find and report fraud.

10. It will never be possible to eliminate all fraud. However, there are a range of **fraud indicators** – both warning signs and fraud alerts (red flags) – which can provide early warning that something is not quite right and increase the likelihood that the fraudster will be discovered.

11. There are also **two key tools for detecting fraud** – training and experience combined with the necessary mindset that fraud is always a possibility. These can be supplemented by a range of techniques for identifying and analysing anomalies to help determine whether further action is required.

12. An organisation should set out its approach to dealing with fraud in its **fraud policy** and **fraud response plan.** Organisations should ensure that this includes provision for learning lessons from fraud incidents and appropriate, prompt follow-up action.

INTRODUCTION

Aim of this guide

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 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 for virtually every type of organisation in every part of the world. 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.

There is a wealth of surveys and research[1] which demonstrate the extent and effect of corporate fraud. Typical findings are that:

- Organisations may be losing as much of 5% of their annual revenues as a result of fraud.
- Small organisations are disproportionately affected by fraud.
- Anti-fraud controls help to reduce the cost and duration of frauds.
- A high percentage of frauds are committed by senior management and executives.
- Fraudsters often work in the finance function.
- Fraud losses are not restricted to a particular sector.
- The prevalence of fraud is increasing in emerging markets.
- The threat of fraud is evolving and organisations which actively manage fraud risk stand to benefit.

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. As one recent survey of 1,265 executives worldwide concluded, "All businesses are confronted with the risk of fraud. How they respond – the nature of their approach to prevention, detection, investigation and disclosure will separate those who manage through the issues from those who suffer significant loss."[2]

This guide aims to help finance professionals and others with an interest in tackling fraud in their organisations to take practical steps towards establishing more robust procedures to tackle fraud, particularly in terms of prevention, detection and response. It is aimed at readers across the world – as the law relating to fraud varies from country to country, we strongly advise readers to ensure that they are familiar with the law relating to fraud in their own jurisdiction. However, the general principles of good fraud risk management are universally applicable and we hope that the emphasis on the practical in this guide will provide plenty of pointers for action.

Also included in the guide are insights from the *2011 AICPA Forensic and Valuation Services (FVS) Trend Survey* of over 1,000 respondents including both forensic accounting practitioners and senior finance professionals in business and industry. This survey explored a number of issues around fraud, including methods of prevention and detection, as well as types of fraud and departments where frauds took place.

What is fraud?

There is no universal definition of fraud. But it essentially involves using deception to make a personal gain dishonestly for oneself and/or create a loss for another.

Examples of fraud include:

- Crimes by individuals against consumers, clients or other business people eg pyramid trading schemes.
- Employee fraud against employers eg payroll fraud, falsifying expenses.
- Crimes by businesses against investors eg selling counterfeit goods.
- Crimes against financial institutions eg fraudulent insurance claims.
- Crimes by individuals or businesses against government eg tax evasion.
- Crimes by professional criminals against major organisations eg money laundering.
- E-crime eg phishing, spamming, hacking.

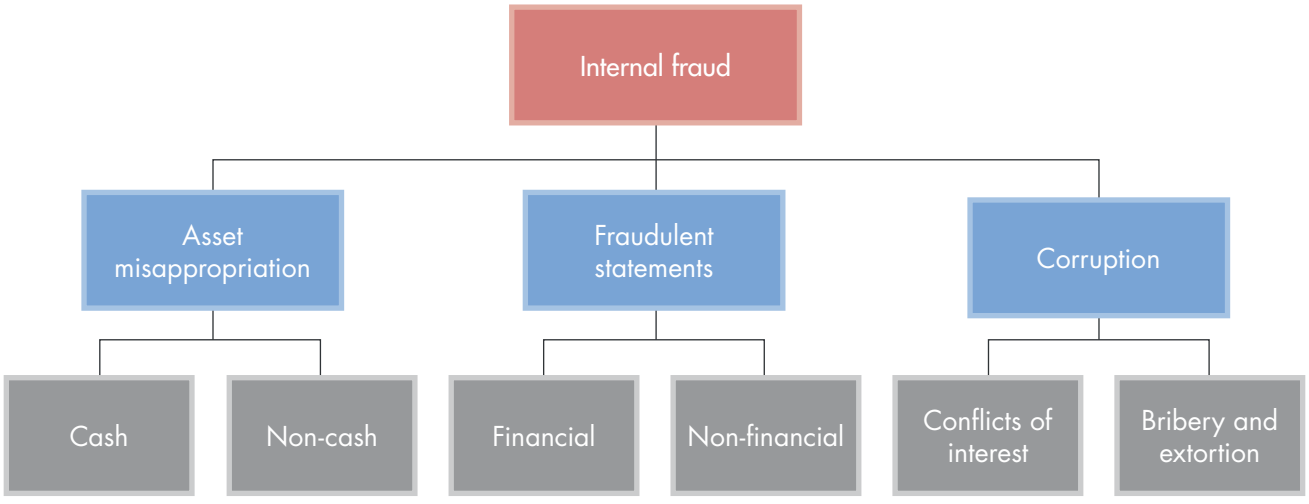
This guide focuses on fraud against businesses, typically by those internal to the organisation. According to the Association of Certified Fraud Examiners (ACFE), there are three main categories of fraud that affect organisations:

- Asset misappropriation, 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.
- Fraudulent statements usually in the form of falsification of financial statements in order to obtain improper benefit. It also includes falsifying documents such as employee credentials.
- Corruption 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 the chart shown in Figure 1.

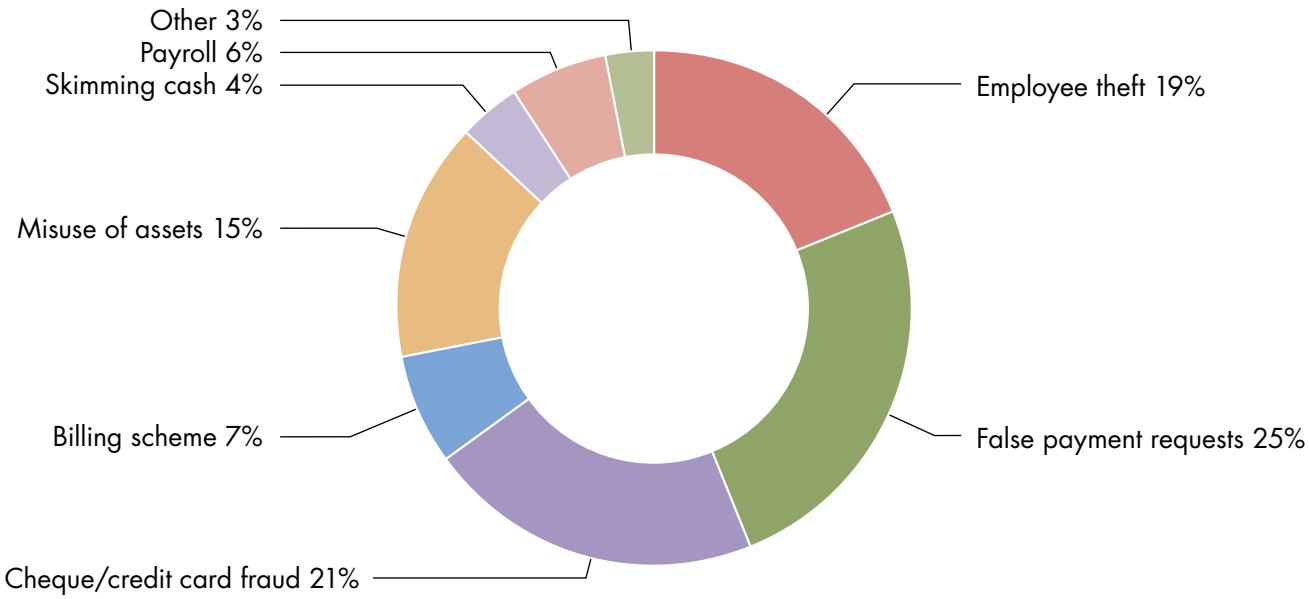
Further information on common types of internal fraud and methods by which they may be perpetrated is included in appendix 1.

FIGURE 1: Types of internal fraud



The *AICPA Forensic and Valuation Services (FVS) Trend Survey* analysed types of fraud occurring as follows:

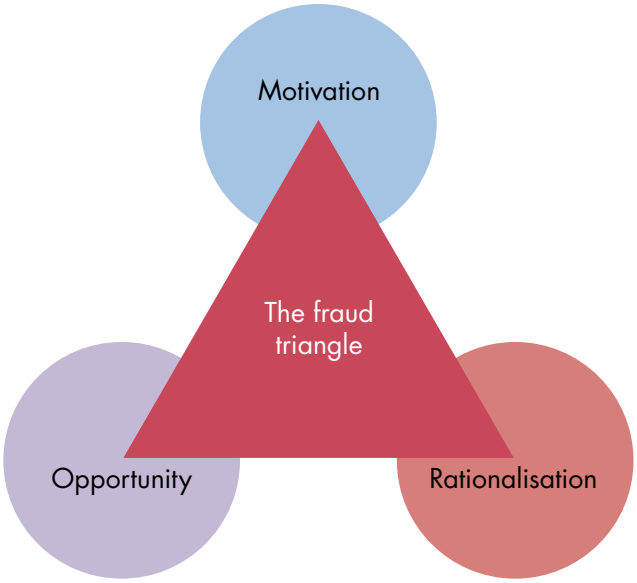
FIGURE 2: Types of fraud that occurred



Why do people commit fraud?

There is no single reason behind fraud. A useful model is the fraud triangle which is based on the premise that fraud is likely to result from a combination of three factors: motivation, opportunity and rationalisation.

FIGURE 3: The fraud triangle



- Motivation – typically based on greed or need, eg resulting from financial difficulties.
- Opportunity – where there are weak internal controls, poor security, little fear of exposure or likelihood of detection.
- Rationalisation – some may rationalise fraudulent actions as necessary, especially when done for the business, harmless because the victim was large enough to absorb the impact or justified because the perpetrator had a sense of grievance.

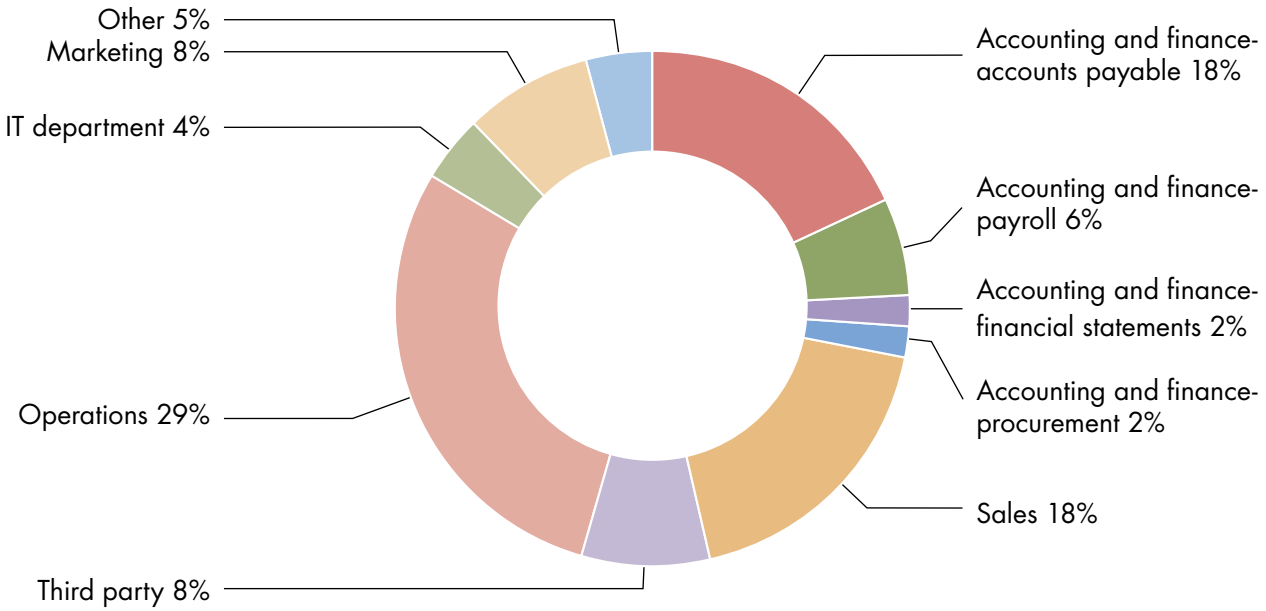
One of the most effective ways to tackle fraud is to adopt methods that will decrease motive and opportunity. Rationalisation is personal to the individual and harder to combat although a strong organisational ethical culture and values can help. These methods and principles are covered in later sections of this guide.

Who commits fraud?

Surveys often show that fraudsters often work in the finance department or operations/sales. This is reflected in the findings of the *AICPA Forensic and Valuation Services (FVS) Trend Survey.*

Another common finding is that senior management and executives commit a significant number of frauds – and invariably cause greater losses than more junior employees.

FIGURE 4: Organisational area where the fraud occurred



FRAUD PREVENTION

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 toward tackling fraud. However, there is sometimes debate as to whether these resources should be committed to fraud prevention or fraud detection.

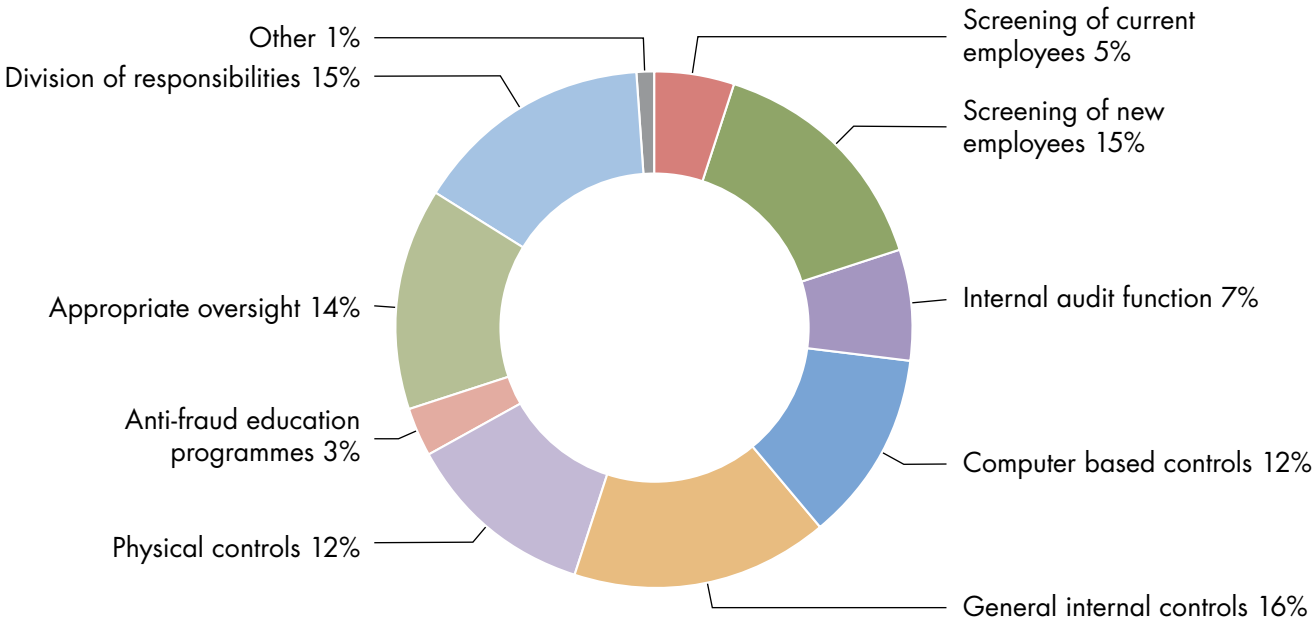
Fraud prevention

One way to deal with fraud is to adopt methods that will decrease motive, restrict opportunity and limit the ability for potential fraudsters to rationalise their actions. 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 as well as activities such as training and fraud awareness to stop fraud from occurring.

It is profitable to prevent losses, and fraud prevention activities can help ensure the stability and continued existence of a business. However, many organisations do not have a formal approach to fraud prevention and once a fraud has occurred, the likelihood of recovering assets can be very low. Prevention is better than cure when it comes to fraud.

The *AICPA Forensic and Valuation Services (FVS) Trend Survey* shows the following breakdown of fraud prevention methods.

FIGURE 5: Fraud prevention methods



However, while worthwhile, fraud prevention methods cannot provide 100% protection. It is difficult to remove all opportunities for perpetrating fraud.

Fraud detection

As fraud prevention techniques cannot be 100% effective, organisations also need to engage in 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
- Ongoing risk assessment.

Fraud detection may identify ongoing frauds that are taking place or that have already occurred. The objective of a detection programme should not be limited to potential recovery of losses. Fraudulent behaviour should not be ignored just because there is no possibility of asset recovery. Fraud detection also allows for improvement of internal systems and controls, which can enhance fraud prevention.

The *AICPA Forensic and Valuation Services (FVS) Trend Survey* shows the following breakdown of fraud detection techniques.

Fraud prevention and detection both have 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

In fact, an effective anti-fraud strategy has four main components:

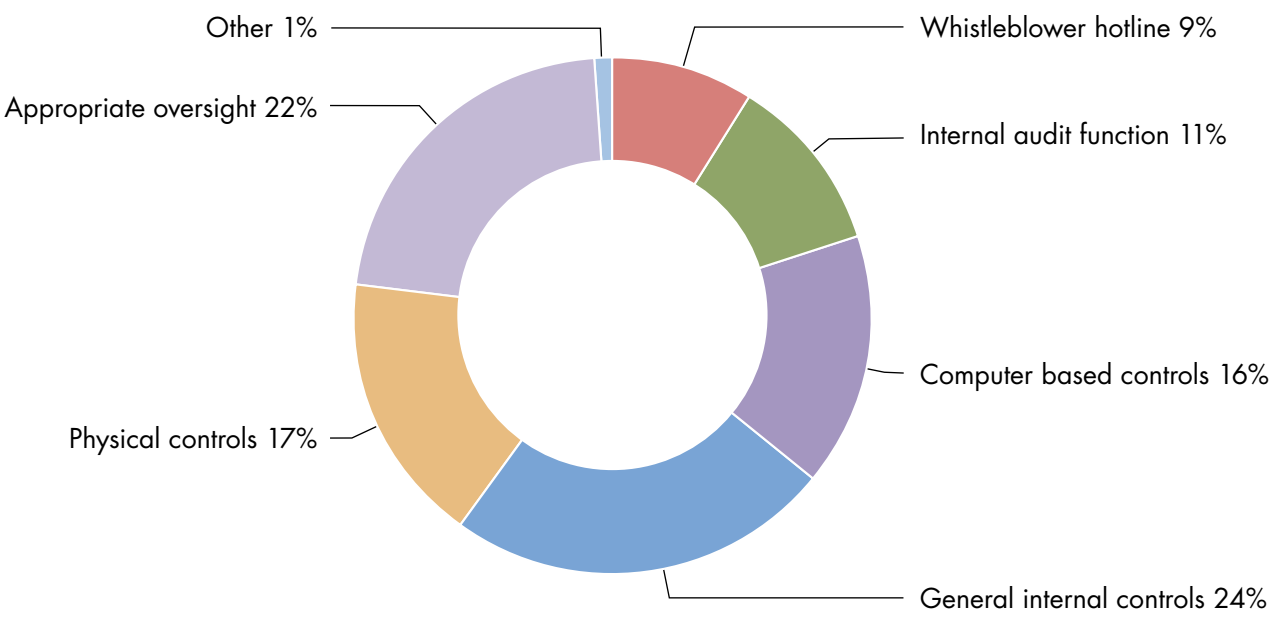
a. Prevention

b. Detection

c. Response

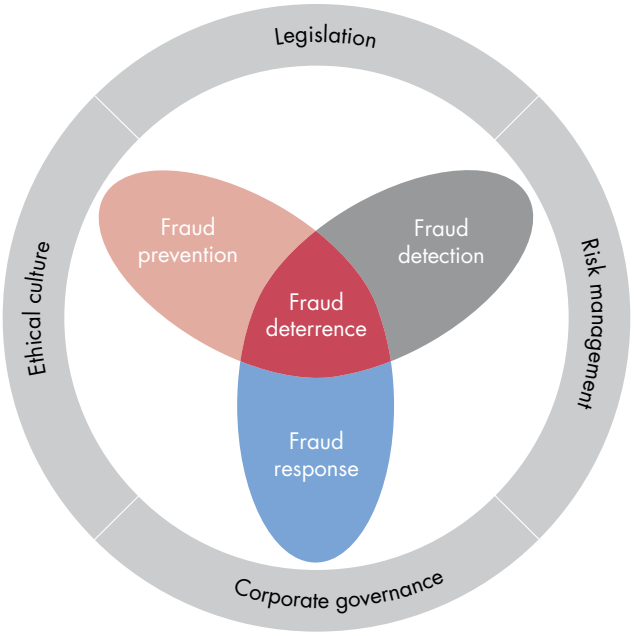
d. Deterrence

FIGURE 6: Fraud detection methods



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

FIGURE 7: Anti-fraud strategy



This shows that the various elements of an effective anti-fraud strategy are closely interlinked and each plays a significant role in combating fraud. It is the combination of effective fraud prevention, detection and response measures that create an effective fraud deterrent.

Fraud detection and response are considered in subsequent sections. Some of the main preventative approaches which can be implemented to minimise the cost and occurrence of fraud are highlighted below. These approaches are generic and can be applied, as appropriate, to different organisations and particular circumstances.

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, such as petty theft, larger frauds committed by senior 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 time to consider where they stand on ethical issues often realise that high ethical standards bring long-term benefits as customers, suppliers, employees and members of the community.

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.

Key actions that organisations can take to establish a sound ethical culture are:

- A mission statement that refers to quality, ethics and how the organisation wishes to be seen 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 in appendix 2).
- A route through which suspected fraud can be reported.
- A process of reminders about ethical and fraud policies.
- An aggressive risk-based audit process.
- Management which is seen to be committed through its actions.

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

To demonstrate commitment, resources should be allocated to:

- communicating ethics and values to all employees, suppliers and business partners.
- providing training programmes where necessary.

In addition to encouraging senior management to set ethical examples by their actions, organisations should ensure that senior management is committed to controlling the risks of fraud. Senior managers 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 handled at a senior level. Adherence to policies and codes should be regularly monitored and policed by appropriate staff within the organisation, such as management and/or internal audit. The documents themselves should also be regularly reviewed and revised.

Periodic assessment of fraud risk

Organisations should regularly identify and assess fraud risks – perhaps as part of an overall risk management process[3]. Fraud risks should be identified for all areas and processes of the business. They should 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 example of a risk analysis is shown in appendix 3.

An effective fraud risk assessment will highlight new risks and strengthen fraud prevention and detection. Opportunities for cost savings may also be identified.

Fraud risk training and awareness

Almost every time a major fraud occurs, many people who were unwittingly close to it, are shocked that they had no idea it was going on. It is therefore important to raise awareness through education and training. Particular attention should be paid to employees working in high risk areas, such as procurement and finance, and to those with a role in the prevention and detection of fraud, for example human resources.

One question often raised is whether fraud training provides employees with the knowledge to commit fraud! However, fraud is often discovered through a tip-off. It is therefore essential that all employees understand what constitutes fraud, how to identify it and how they should respond. On balance, training is more likely to reduce rather than increase the risk of fraud.

Training methods may include:

- formal training sessions
- group meetings
- posters, employee newsletters and Intranet content.

Communication should be ongoing and a combination of methods is usually most successful.

Spending money on preventing fraud brings many benefits – but there can be downsides, for example, 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 whistle-blowing

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 others who are not involved. The challenge for organisations is to encourage such employees to speak out and to demonstrate that it is in their own best interest.

There may be many conflicting emotions influencing the potential 'whistle-blower':

- 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 whistle-blower, as it is often fear of the consequences, which has the greatest impact. To the whistle-blower, the impact of speaking out can be traumatic, ranging from being dismissed to being shunned by other employees.

Where fraud is committed by senior management – even the Chief Executive, the predicament faced by the whistle-blower is exacerbated. This is where the greatest challenge lies – to convince staff that every employee 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 are likely to benefit in many ways, for example, in being able to detect potential problems early and to ensure that the critical information gets to the right people at the right time to enable them to address issues effectively.

While many countries have legislation in place to protect whistle-blowers, legal redress should be a last resort and organisations should strive for a culture that actively encourages employees to speak up and challenge inappropriate behaviour. It is also essential that the organisation follows up any disclosures. Employees are more likely to speak up if they know that action will be taken in response.

A whistle-blowing policy should also make provision for anonymous reporting. In some cases, for example, companies subject to the Sarbanes-Oxley Act are required to do this, but it may be necessary to be aware of relevant data protection legislation, for example, companies operating in Europe must comply with EU rules that state that personal data should only be collected fairly. To cover the breadth of whistle-blowing legislation across the world is beyond the scope of this report and readers are strongly advised to verify the specific situation in their own jurisdiction before establishing a whistle-blowing policy and to share useful information sources with other CGMAs via the CGMA community website at **www.cgma.org**. A sample whistle-blowing policy is shown in appendix 4.

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'.

Overall responsibility for the organisation's system of internal control must be at the highest level in the organisation.

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, pre-employment screening and physical security. These procedures often include the division of responsibilities as well as checks and balances to reduce risk.

Ultimately, the internal control system should be embedded within the culture and operations of the organisation. It should also be consistent with the nature and size of the organisation.

Internal controls to minimise fraud should address fraud red flags. Examples of controls may be:

- Requiring multiple signatories on high value transactions.
- Requiring employees to take holiday (this is common in the banking sector).
- Restricting belongings that can be brought into the work environment eg USB sticks.
- Conducting random searches of employees eg in retail outlets.

A widely used framework is COSO's *Internal Control – Integrated Framework* which provides principles-based guidance for developing and implementing effective internal controls.[4] This is currently being updated for release in 2012 to mark the 20th anniversary of the publication of the current version. It is the most widely used framework in the US and has been adopted or adapted by numerous countries and businesses across the world.

The COSO framework defines internal control as a 'process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives' in three categories:

1. Effectiveness and efficiency of operations.
2. Reliability of financial reporting.
3. Compliance with applicable laws and regulations.

A sound ethical culture and effective system of internal control are essential elements of an anti-fraud strategy. However, neither can provide complete protection against all fraudulent behaviour, highlighting the importance of fraud detection measures.

Appendix 5 provides an example of a 16 step fraud prevention plan that brings together many of the elements described in this section.

FRAUD DETECTION

Detection methods

It is interesting to look at how most frauds are actually detected.

The *PwC 2011 Global Economic Crime Survey*,[5] covering 3,877 respondents from 78 countries established that the most prevalent fraud detection methods in reported cases of fraud were:

- Internal audit (14% of respondents said that frauds were detected by internal audit).
- Internal tip-off (11%) – but only 5% of respondents said frauds were uncovered via whistle-blowing mechanisms.
- Fraud risk management measures (10%).
- By accident (8%).

The *AICPA Forensic and Valuation Services (FVS) Trend Survey* shows a relatively similar picture.

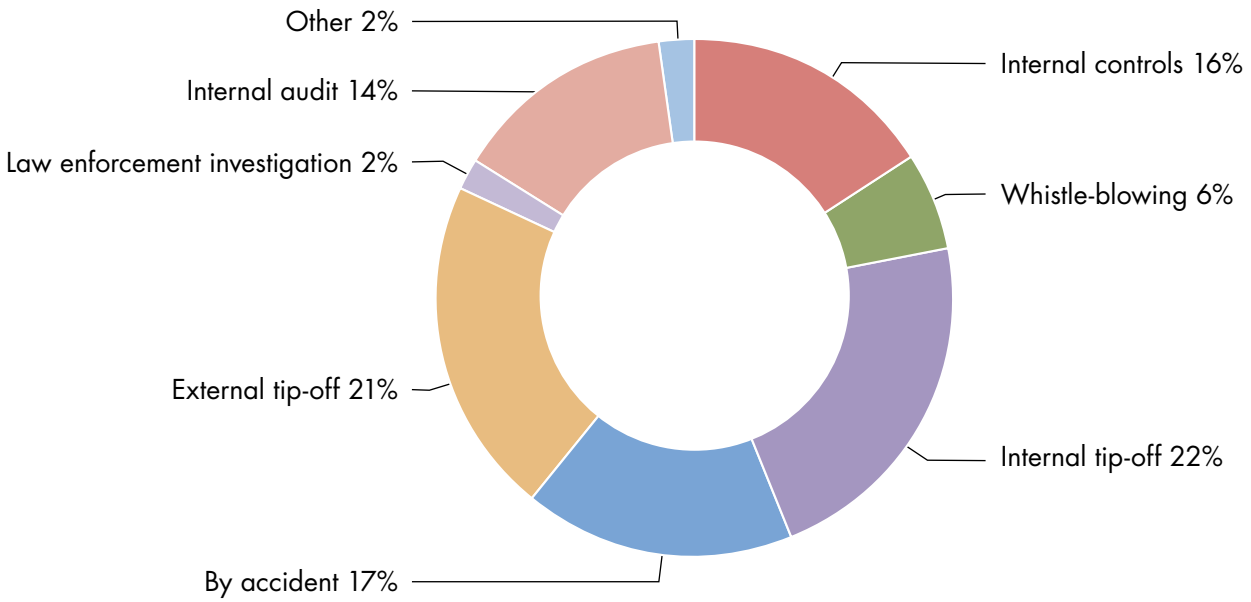
In both cases, a striking feature is the number of frauds that are uncovered either accidentally or as a result of tip-offs. This reinforces the importance of raising general fraud awareness in the organisation and emphasising that it is everyone's responsibility in the organisation to find and report fraud. It is also essential that there are adequate controls and reporting mechanisms to facilitate this activity.

However, the PwC survey also noted changing trends in fraud detection, with the number of economic crimes detected by people (eg tip-offs) going down and those detected by computers going up. PwC therefore fears that this could mean more fraud overall going undetected as headcounts fall in control functions.

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.

FIGURE 8: Fraud detection methods in identified cases



Fraud indicators fall into two categories:

- warning signs
- fraud alerts.

Warning signs

These are organisational indicators of fraud risk and some examples are set out below. Further examples can be found in appendix 6.

Business risk

Cultural issues

- Absence of 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/external auditors.
- Lack of management supervision of employees.
- 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 employee behaviour patterns.
- Personal financial pressures on key employees.
- Low salary levels of key employees.
- 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.

External risk

- Introduction of new accounting or other regulatory requirements, including health and safety or environmental legislation, which could alter reported results significantly.
- Highly competitive market conditions and decreasing profitability levels within the organisation.
- The organisation is 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

- Major information threats include: mobile devices, malicious insiders, remote access and social media.
- 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 eg 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

These are 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.

Fraud alerts

- 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.

Tools and techniques

Two key tools are:

- Training and experience – the training received by a management accountant is a very good basis for implementing an anti-fraud programme. The broad understanding of business processes is an important asset as is the 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 the management accountant develops with experience.
- The mindset that fraud is always a possibility. A healthy dose of professional scepticism should be maintained when considering the potential for fraud.

There are also useful techniques to help identify and analyse anomalies which may be fraud. These should be monitored and updated regularly. For example, the *AICPA Forensic and Valuation Services (FVS) Trend Survey* revealed that most respondents cited improvements in computer based controls as a key area for improving both fraud prevention and detection over the next two to five years.

Identifying anomalies

Background reading

- It is important to keep up to date with fraud trends and issues through the press, technical journals, books and the internet.

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 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 Benford's Law, a formula which can help identify irregularities in accounts. Database modelling can also be used.

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 predetermined threshold values (exceptions), enabling immediate identification of results deviating from the norm. Emails or text alerts can be sent directly to appropriate managers to follow up.

Analysing anomalies – a systematic approach

This can help determine whether further fraud investigation or review is required.

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 actual practice with those in the procedures manual, can help to identify system or procedural failures.

3. Establish the scale of risk

This involves identifying the potential loss and assessing whether it is material.

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.

6. Prepare schedules

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.

7. Prepare the report

In preparing the report, bear in mind that, whatever the original objective, there is always the possibility of it being used in evidence in legal proceedings. The report should be as 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.

FRAUD RESPONSE

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 included in appendices 7 and 8 respectively. Appendix 8 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 section relate to those in the outline fraud response plan in appendix 7.

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 should provide procedures 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 legal action.

Other benefits of the 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
- help ensure the integrity of the evidence.

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.

One question to consider is publicity relating 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.

In some industries, for example the regulated financial services industry, there are often legal requirements to report financial crime. Other businesses should follow this example and make it clear that they will not sweep fraud under the carpet.

Definition of fraud

The plan should provide a clear explanation of activities which would or could be considered fraudulent. Where appropriate, it could also provide for legal definitions.

Roles and responsibilities

The division of responsibilities for fraud risk management will vary between organisations, depending on size, industry, culture and other factors. The following are some general guidelines which can be adapted to suit specific circumstances.

General management

- Should take responsibility for detecting fraud in their departments.
- Ensure their staff report any suspected irregularities.
- Should be provided with a response card, detailing how they should respond to a reported incidence of fraud. This should include a list of appropriate contacts.

Finance Director/Chief Financial Officer

- Will often have overall responsibility for the organisation's response to fraud, including responsibility for coordinating investigations and keeping the fraud response plan up to date.
- Will hold the master copy of the fraud response plan.
- Responsible for maintaining an investigation log, which details all reported suspicions, including those dismissed as minor or otherwise not investigated. It will also contain details of actions taken and conclusions reached. An important tool for managing, reporting and evaluating lessons learnt.

Fraud Officer (where applicable)

- May be appropriate to designate a senior manager as Fraud Officer instead of the CFO – especially in larger organisations.
- Should be authorised to receive enquiries from employees confidentially and anonymously.
- Should have authority to act and/or provide advice according to individual circumstances, and without recourse to senior management for approval.
- Where the suspect is more senior than the Fraud Officer, reports should be made to another senior manager or non-executive director, ideally the Chairman of the Audit Committee.

Human resources

- Usually responsible for any internal disciplinary procedures, which must be in line with the fraud response plan.

Audit committee [6]

- Has an active role to play in the prevention and detection of fraud. In some countries, this role has been reinforced by recent legislative and regulatory change.
- Typically, audit committees have responsibility for reviewing the organisation's internal control systems, including the design, implementation and effectiveness of anti-fraud programmes and controls.
- Also have responsibility for ensuring that the organisation has whistle-blowing arrangements in place and that these are effective.
- The audit committee will also need to oversee the effectiveness of both the internal and external auditors in performing their respective responsibilities in relation to fraud.

Internal audit

- Likely to investigate any incidence of fraud.
- 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 audit

- An organisation without its own internal audit function may consider consulting its external auditors if it discovers 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 a specialist fraud investigation team.
- A decision to call in 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

- Can provide technical advice on IT security, capability and access.
- If computers have been used to commit the fraud, or if they are required for evidence, 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 if the fraud becomes public knowledge. Alternatively, an organisation may decide that it is in its best interests to be proactive and make a public statement before news leaks out.

Police

- If it is in the organisation's policy to prosecute all those suspected of fraud, the police should be involved at the outset of any investigation, as any delay could reduce the chances of success.

External consultants

- Organisations can consider using specialist investigation skills from outside the organisation such as forensic accountants.
- Many specialist organisations 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 insurers, and any additional requirements, should be included in the fraud response plan and is usually specified in the insurance document.

The response

Reasonable steps for responding to detected or suspected instances of fraud include:

- Clear reporting mechanisms.
- A thorough investigation, using forensic accountants.
- 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 future.

Reporting suspicions

- Procedures should be set out clearly and succinctly.
- This may be by means of a formal whistle-blowing policy – see Fraud prevention section – but the procedures should also be summarised in the fraud response plan.

Establish an investigation team

- After recording details of the allegations, the Finance Director/CFO, 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 along with resources required, the scope of the investigation and the timescale.
- The objectives 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 as well as protocols for handling and recording evidence should be clearly understood by everybody.

The investigation

Preservation of evidence

- A key consideration must always be how to secure and preserve 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 alerted.
- If an individual is subsequently charged with a criminal offence, all investigations, and relevant evidence arising from such investigations, will be open to discovery, by the 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 section 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, an organisation has a right to access its own records and may bring disciplinary action against any employee 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 seize 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 physical evidence, original material is essential. Photocopies are not acceptable.
- Records should be kept of when the evidence was obtained and the place that it was taken from.
- If evidence consists of several items, eg a number of 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

- Retrieval of electronic evidence should be generally treated in a similar manner to that of other physical evidence, although there will be some distinct differences. It is essential to check the current legal position with respect to electronic evidence, but the following principles from the UK Association of Chief Police Officers provide a useful starting point:
- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may be relied on in court.
- 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 implications of their actions.
- An audit trail 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.
- The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Interviews

- Managers are entitled to interview their immediate employees 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 supervision of other 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 subject of a formal investigation.
- From this point onwards, any interviews should be conducted by trained staff or by police officers – see Statements from suspects section.
- 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 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 manager usually helps to confine the statements to the relevant facts.
- The witness should be given the opportunity to be supported by a colleague or union official.

Statements from suspects

- If a criminal act is suspected, it is essential that legal requirements are considered before an interview with a suspect takes place, since compliance will usually determine whether evidence is admissible in criminal proceedings.
- In practice, therefore, it is recommended that interviews should only be conducted by specially trained managers, with advice and guidance from the organisation's legal advisers and police.

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:

- Internal disciplinary action.
- A civil response whereby action is taken through the courts to recover losses.
- Criminal prosecution.
- A parallel response where both a civil response and criminal prosecution are pursued.

Follow up action

- There are lessons to be learned from every identified incident of fraud.
- The organisation's willingness to learn from experience is as important as any other response.
- Large organisations may consider establishing a special review to examine the fraud with a view to recommending improvements to systems and procedures.
- Smaller organisations may consider discussing the issues with some of its more experienced people, with the same objectives in mind.
- It is important that recommended changes are implemented promptly.

Appendix 1

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 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 (eg partial shipments, soft sales, contracts with multiple deliverables, upfront 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 (eg 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 eg 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 join 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 (eg customs officials, tax inspectors).
- Anti-trust activities such as price fixing or bid rigging.
- Illegal political contributions.

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 2

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 employees 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 and corruption. These documents give a framework for a response as well as 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 investigation 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 employees 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 committed to maintaining an honest, open and ethical culture 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. For these purposes, 'reasonably held suspicions' shall mean any suspicions other than those which are shown to be both raised maliciously and then found to be groundless.

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 impact column 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 of contracts	Date of assessment	Probability/ likelihood	Impact	Controls impact	Net likely impact	Action
Unchanging list of preferred suppliers	2010	High	High	Low	High	Priority – immediate
Consistent list of single source suppliers	2010	Medium	High	High	Medium	–
Changes in contract specifications	2010	Low	Low	Medium	Low	–
Personal relationships between staff and suppliers	2011	Low	High	Low	High	Priority – within six months

Appendix 4

Sample whistle-blowing policy.

Introduction

This whistle-blowing policy provides a procedure which enables employees to raise concerns about what is happening at work, particularly where those concerns relates to unlawful conduct, financial malpractice or dangers to the public or the environment. The objective 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 whistle-blowing 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 he or she is mistaken.

How the whistle-blowing 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 whistle-blowing policy is primarily concerned with situations where the interests of others or the organisation are at risk. It may be difficult to decide whether a particular concern should be raised under the whistle-blowing policy or under the grievance procedure or 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 whistle-blowing 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 (eg if the employee's evidence is needed in a court of law), the best way to proceed with the matter will be discussed with the employee. Employees may submit reports anonymously, but should be aware that doing so, it will be more difficult for the organisation to investigate them, to protect the employee and to give the employee feedback.

How the matter will be handled

Once an employee has informed the organisation of his or her concern, these 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 advised 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 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 whistle-blowing telephone hotline. This service is strictly confidential and callers will not be asked to give their name if they do not wish to do so.

Step 2

If these channels have been followed and the employee still has concerns, or feels that they are unable to raise the issue with their line manager, for whatever reason, they should address their concerns to their head of department, the head of human resources or the chief internal auditor [OR INSERT OTHER APPROPRIATE NOMINATED POINTS OF CONTACT HERE].

Anonymous reports

These may be made verbally to the 24 hour whistle-blowing telephone hotline or in writing to [INSERT NOMINATED POINT OF CONTACT SUCH AS HEAD OF HUMAN RESOURCES OR CHIEF INTERNAL AUDITOR].
The submission should be clearly marked 'Confidential: anonymous employee submission'.

Independent advice

If an employee is unsure whether to use this procedure, to report the matter externally to regulators/ law enforcement authorities or simply wants independent advice at any stage, they may contact
[INSERT EXTERNAL CONTACT IF APPLICABLE – IN SOME JURISDICTIONS, THERE ARE ORGANISATIONS WHICH CAN PROVIDE FREE CONFIDENTIAL ADVICE TO EMPLOYEES ABOUT MALPRACTICE AT WORK.]
An employee can also seek advice from a lawyer of their own choice at their own expense.

Matters raised maliciously

Employees who are found to raise a matter maliciously that they know to be false, will be subject to the organisation's disciplinary policy.

Appendix 5 – 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 throughout 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, J Finn and D Cafferty, *Financial Management,* September 2002

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 the section 'Fraud detection'.

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 employees 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 company 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 tenderers can have no excuse that they were unaware of the client's policy should fraudulent activity come to light.

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.
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.
Contract 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 contractor 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 contracts 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 prior to opening?
- Who had access to the keys/combination?
- If no tender cabinet used, 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 chairman?
- Confirm that tender lists show no evidence of patronage or incestuous relationships.
- Confirm that companies 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 can also exist in the selling process. Those involved can include any combination of the clients' management or employees and the organisation's own management or employees 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 – outline fraud response plan

1. Purpose of the fraud response plan
2. Corporate policy
3. Definition of fraud
4. Roles and responsibilities
    a. Managers and supervisors
    b. Finance Director/Chief Financial Officer
    c. Fraud Officer
    d. Human resources
    e. Audit committee
    f. Internal auditors
    g. External auditors
    h. Legal advisers
    i. IT
    j. Public relations
    k. Police
    l. External consultants
    m. Insurers
5. The response
    a. Reporting suspicions
    b. Establish an investigation team
        i. Objectives
        ii. Reporting procedures
        iii. Responsibilities
        iv. Powers
        v. Control
    c. Formulate a response
        i. In accordance with corporate policy
6. The investigation
    a. Preservation of evidence
    b. Physical evidence
    c. Electronic evidence
    d. Interviews (general)
    e. Statements from witnesses
    f. Statements from suspects
7. Organisation's objectives with respect to fraud
    a. Internal report
        i. No further action
        ii. Disciplinary action
    b. Civil response
        i. Legal advisers' control
        ii. Legal submissions
        iii. Case file
    c. Criminal response
        i. Police controlled
        ii. Case file
    d. Parallel response
        i. Civil recovery
        ii. Criminal prosecution
8. Follow up action

Appendix 8

Example of a fraud response plan. This example has been based on a response plan used by an organisation within the UK's National Health Service. However, the principles on which it is based are very general and the response plan is therefore applicable to organisations in any sector or location.

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 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 legal action. This document is not intended to provide direction on fraud prevention.

2. Corporate policy

The board is committed to maintaining an honest, open and ethical culture 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. The organisation has a published whistle-blowing 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 definition of fraud

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:

a. The value of the organisation has suffered or may have suffered.

b. Has been misrepresented for personal gain.

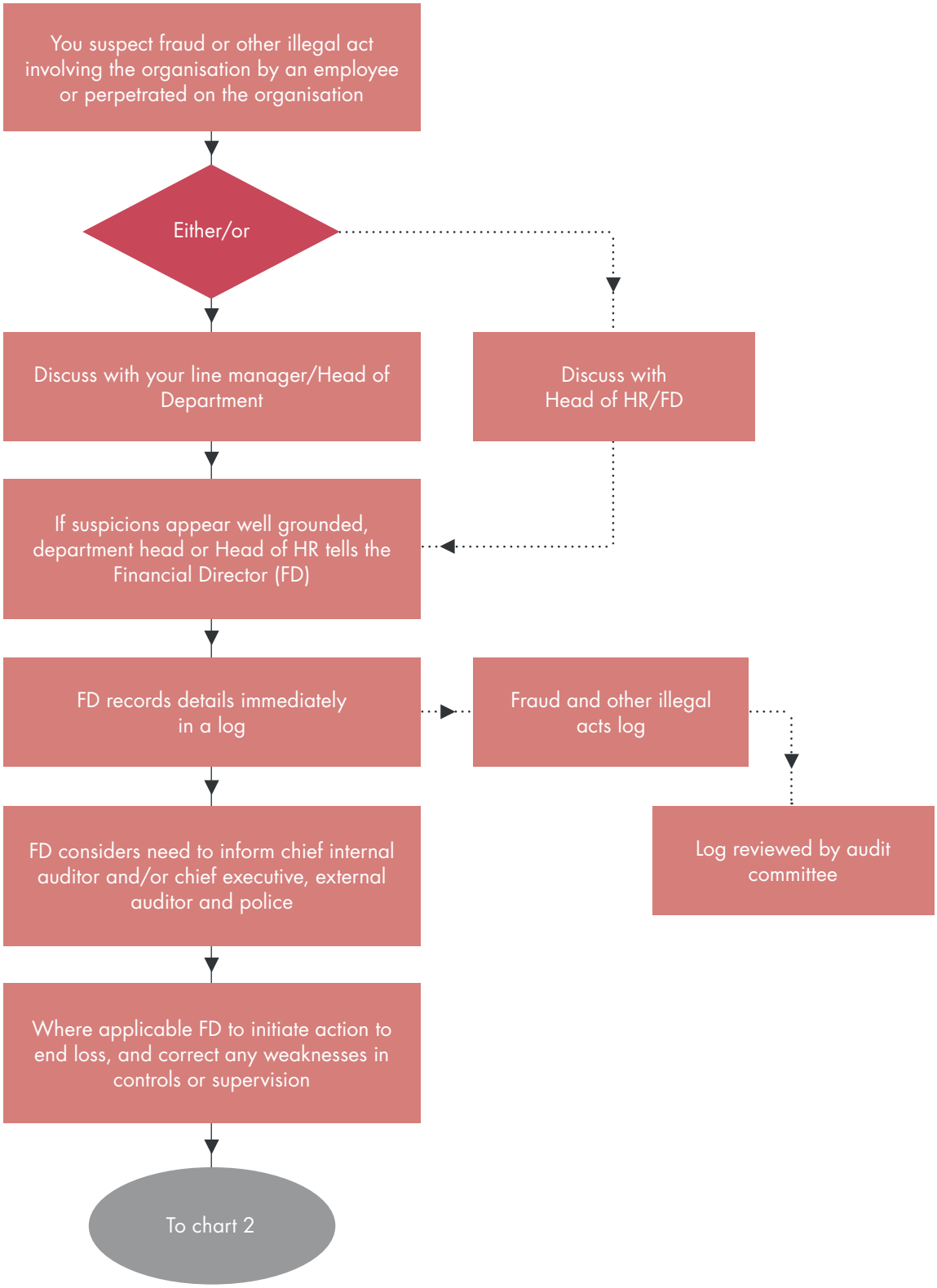
As a result of the actions or omissions of:

c. Directors and employees of the organisation.

d. Customers, contractors and other external stakeholders.

4. Roles and responsibilities

CHART 1: Reporting fraud



Finance Director/CFO

Responsibility for investigating fraud has been delegated to the finance director. Where appropriate/necessary, he/she 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 practicable.

Chief Internal Auditor

The chief internal auditor will:

a. Initiate a diary of events to record the progress of the investigation.

b. Agree the objectives, scope and timescale of the investigation and resources required with the finance director at the outset of the investigation.

c. Ensure that proper records of each investigation 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 an employee 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 (HR).

The Head of HR will advise those involved in the investigation in matters of employment law, company policy and other procedural matters (such as disciplinary or grievance procedures) as necessary.

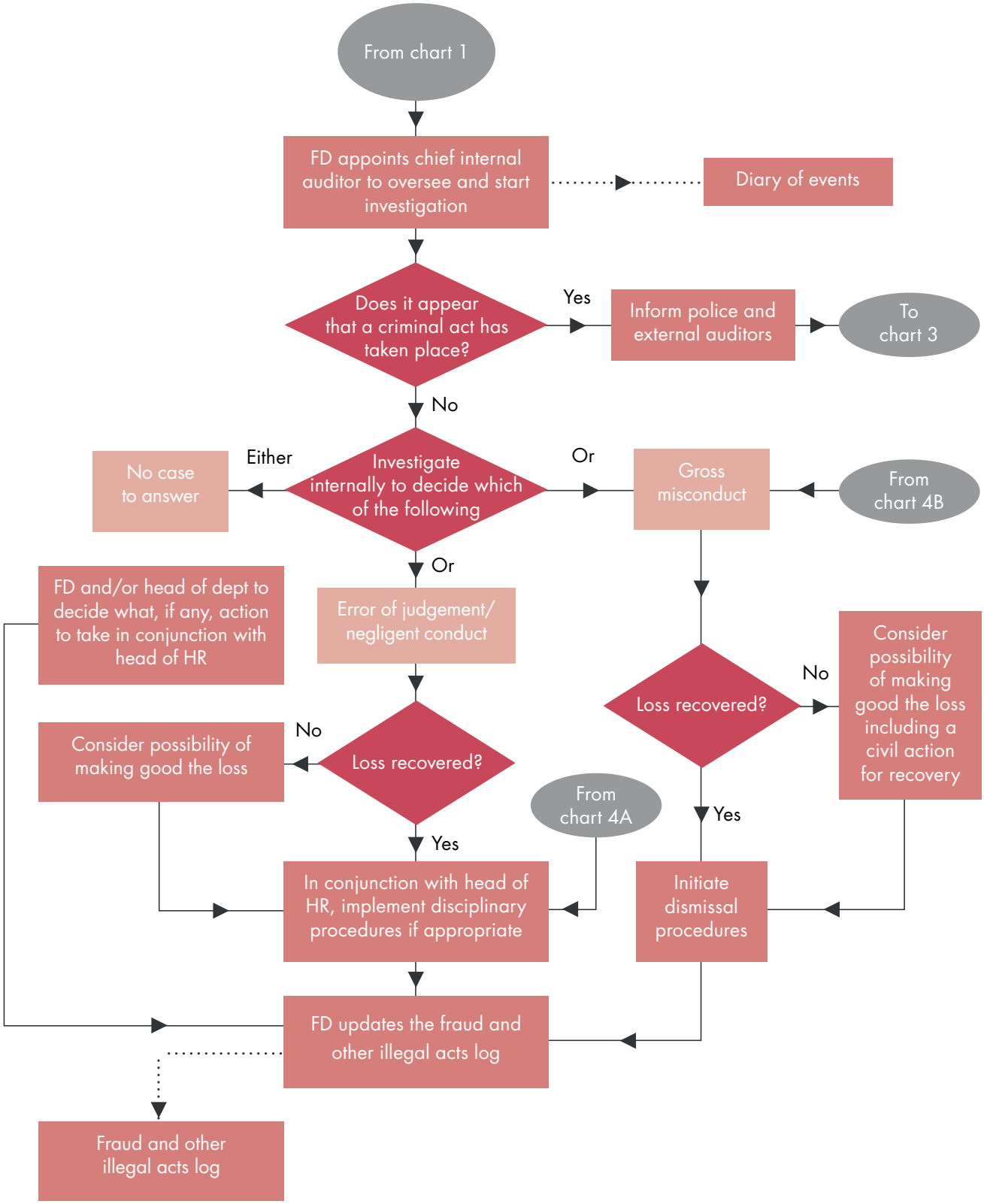
Line and other managers

If, in accordance with the organisation's whistle-blowing policy, an employee raises a concern with their line manager, head of department or the Head of HR, the details must be passed to the finance director immediately for investigation. If a concern involves the finance director, the matter should be reported directly to the audit committee.

Employees

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

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:

a. Determine the facts.

b. Consider what, if any, action should be taken against those involved.

c. Consider what may be done to recover any loss incurred.

d. 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 the 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 an employee and it is determined that no criminal act has taken place, the finance director will liaise with the Head of HR and appropriate line manager to determine which of the following has occurred and therefore whether, under the circumstances, disciplinary action is appropriate:

a. Gross misconduct (ie acting dishonestly but without criminal intent).

b. Negligence or error of judgement.

c. 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 in respect of 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 immediately. 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 a decision on whether a criminal prosecution should be pursued.

Where appropriate, the Finance Director will consider the possibility of recovering losses from the organisation's insurers.

6. The response

CHART 3: Gathering evidence

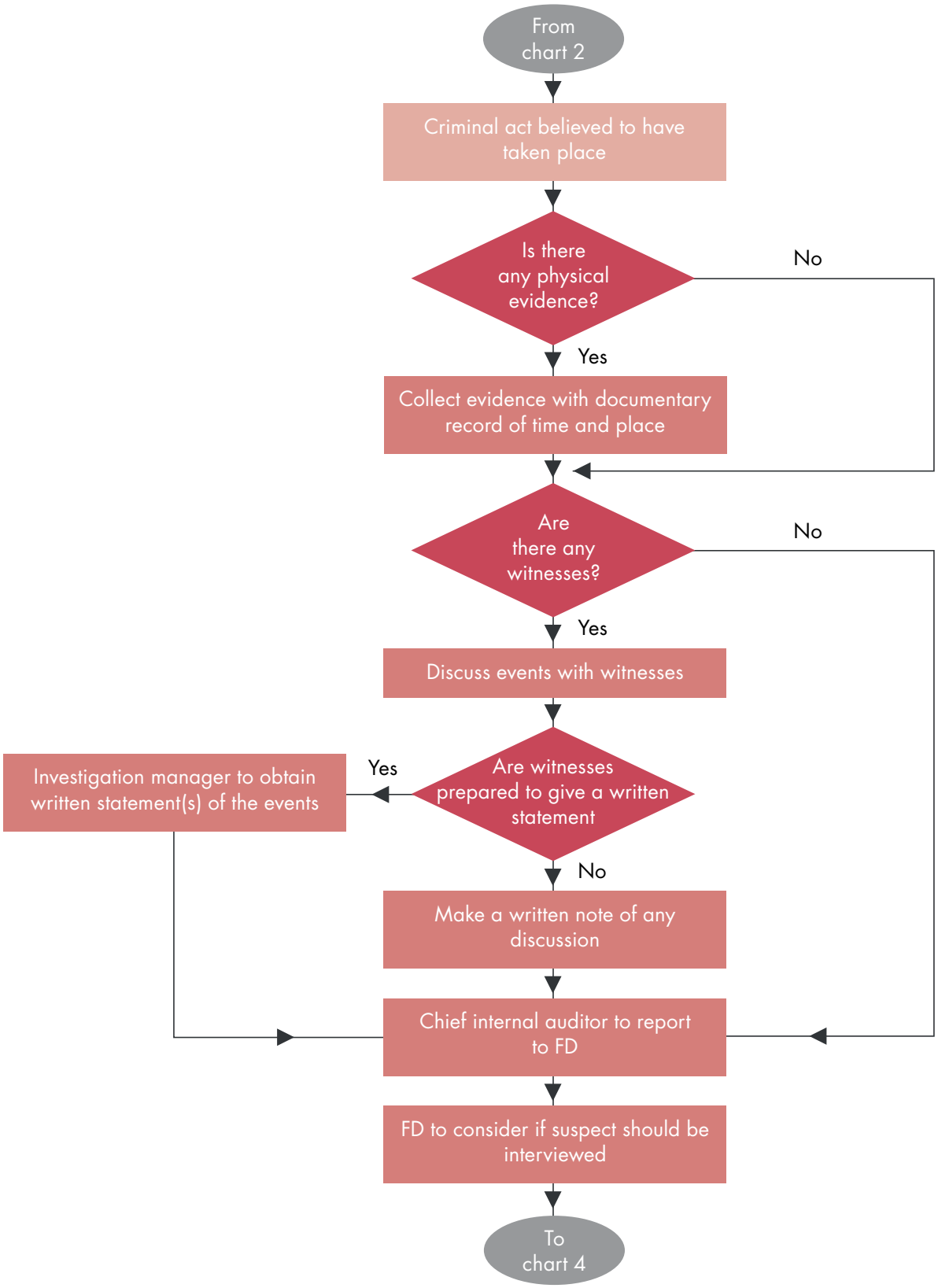
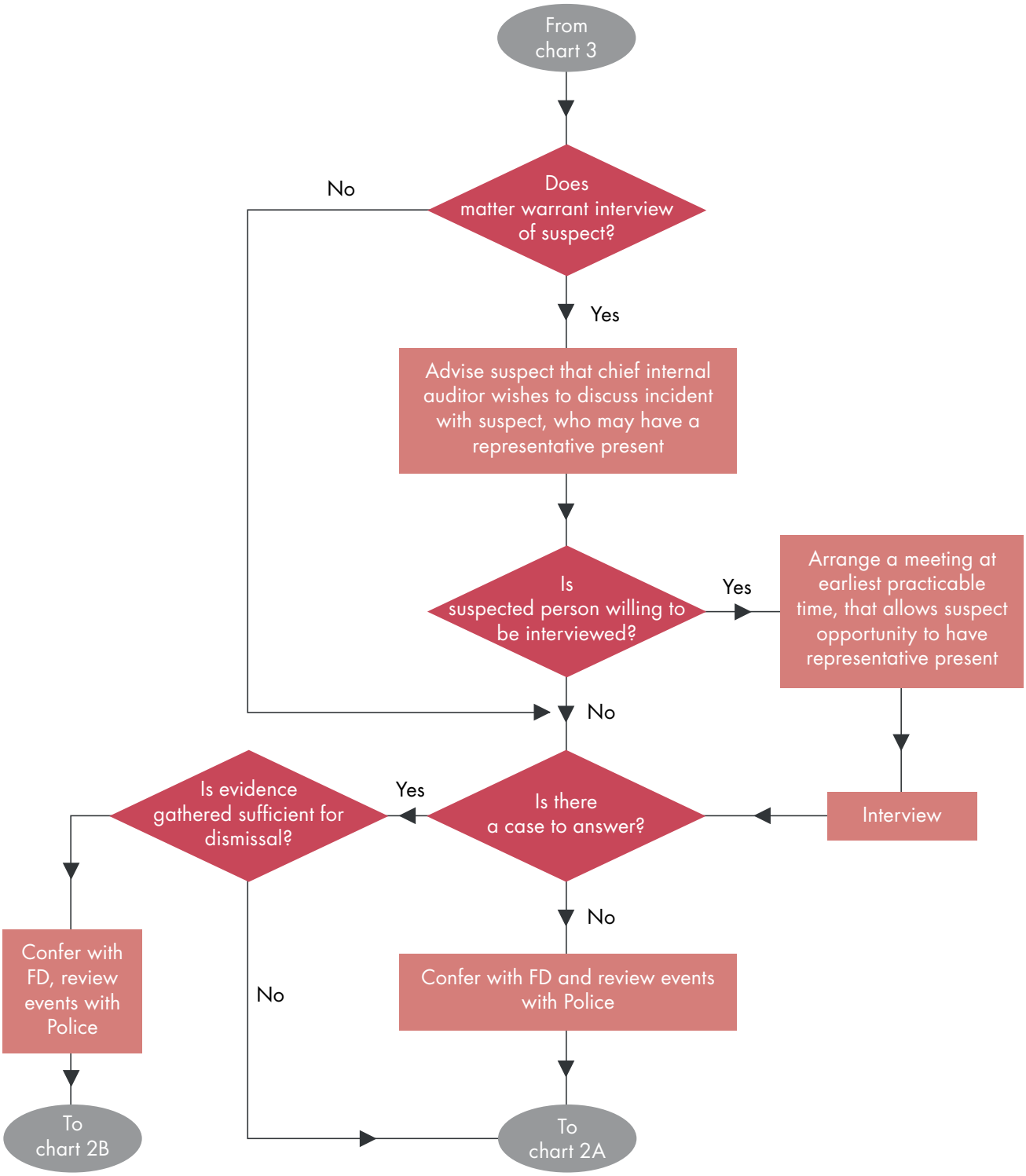


CHART 4: Interview procedure



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. S/he should also ensure that electronic evidence is handled appropriately.

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 eg Head of HR, the Chief Executive and the police before deciding 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 HR. 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 that they 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 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 will be 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 external auditors.

Footnotes

1. Examples include *Report to the Nations on Occupational Fraud and Abuse,* Association of Certified Fraud Examiners, **www.acfe.com**, PwC *Global Economic Crime Survey,* **www.pwc.com**, Kroll and the Economist Intelligence Unit, *Global Fraud Report,* **www.kroll.com**

2. Kroll/EIU *Global Fraud Report Annual Edition* 2011/12, **www.kroll.com**

3. An example is the COSO Enterprise Risk Management Framework. COSO is The Committee of Sponsoring Organizations. It consists of the AICPA, the Institute of Management Accountants (IMA), the Institute of Internal Auditors (IIA), Financial Executives International (FEI) and the American Accounting Association (AAA). The COSO publication *Enterprise Risk Management – Integrated Framework* can be purchased through the AICPA store at **www.cpa2biz.com**. The proceeds from the sale of the framework are used to support the continuing work of COSO.

4. The COSO publication *Internal Control – Integrated Framework* can be purchased through the AICPA store at **www.cpa2biz.com** The proceeds from the sale of the framework are used to support the continuing work of COSO.

5. Cybercrime: protecting against the growing threat, *Global Economy Crime Survey,* PwC, 2011, **www.pwc.com**

6. For additional background on the role of the audit committee in relation to fraud, see The *AICPA Audit Committee Toolkit* – available from **www.cpa2biz.com**.

Acknowledgements

This report is a revised and abridged version of *CIMA's Fraud risk management: a guide to good practice* (2nd edition), CIMA, 2008. CIMA would like to thank all those who contributed to either the first or second editions of the original guide.

ISBN: 978-1-85971-740-0 (Hard copy)
ISBN: 978-1-85971-730-1 (PDF)

American Institute of CPAs
1211 Avenue of the Americas
New York, NY 10036-8775
T. +1 2125966200
F. +1 2125966213

Chartered Institute of
Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom
T. +44 (0)20 7663 5441
F. +44 (0)20 7663 5442

www.cgma.org

January 2012

CIMA has offices in the following locations: Australia, Bangladesh, Botswana, China, Ghana, Hong Kong SAR, India, Ireland, Malaysia, Nigeria, Pakistan, Poland, Russia, Singapore, South Africa, Sri Lanka, UAE, UK, Zambia, Zimbabwe.

Association of International
Certified Professional Accountants

AICPA | CIMA

The Association of International Certified Professional Accountants, a joint venture of AICPA and CIMA, established the CGMA designation to elevate the profession of management accounting globally.