Corporate fraud

About Topic Gateways

Topic Gateways are intended as a refresher or introduction to topics of interest to CIMA members. They include a basic definition, a brief overview and a fuller explanation of practical application, and finally signpost some further resources for detailed understanding and research.

Topic Gateways are available electronically to CIMA Members only in the CPD Centre on the CIMA website, along with a number of electronic resources.

About the Technical Information Service

CIMA supports its members and students with its Technical Information Service (TIS) for their work and CPD needs.

Our information specialists and accounting specialists work closely together to identify or create authoritative resources to help members resolve their work related information needs. Additionally, our accounting specialists can help CIMA members and students with the interpretation of guidance on financial reporting, financial management and performance management, as defined in the *CIMA Official Terminology* 2005 edition.

CIMA members and students should sign into My CIMA to access these services and resources.

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
E. tis@cimaglobal.com
www.cimaglobal.com

Corporate fraud

Definition

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

The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion.

Context

In the current CIMA syllabus, students will study and may be examined on fraud in Paper 3, Management accounting risk and control strategy.

Related concepts

Corporate governance; risk management; internal control; information systems control.

Overview

Surveys are regularly carried out to estimate the true scale and cost of fraud to business and society. While findings vary and it is difficult to ascertain the full extent of fraud, all surveys indicate that fraud is prevalent within organisations and remains a serious and costly problem. Fraud may even be increasing due to greater globalisation, more competitive markets, rapid developments in technology and periods of economic difficulty.

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. No system is completely fool proof, but business can take steps to deter fraud and make it much less attractive to commit. Management accountants, whose professional training includes information and systems analysis, have a significant role to play in developing and implementing anti-fraud measures within their organisations.

There are many types of corporate fraud, including the following common frauds:

- theft of cash, physical assets or confidential information
- misuse of accounts
- procurement fraud
- payroll fraud
- financial accounting mis-statements
- inappropriate journal vouchers
- suspense accounting fraud
- fraudulent expense claims
- false employment credentials
- bribery and corruption.

This topic gateway focuses on fraud perpetrated by those internal to the organisation. Businesses are also susceptible to fraud committed by outsiders, such as corporate identity theft, intellectual property fraud or cyber crime.

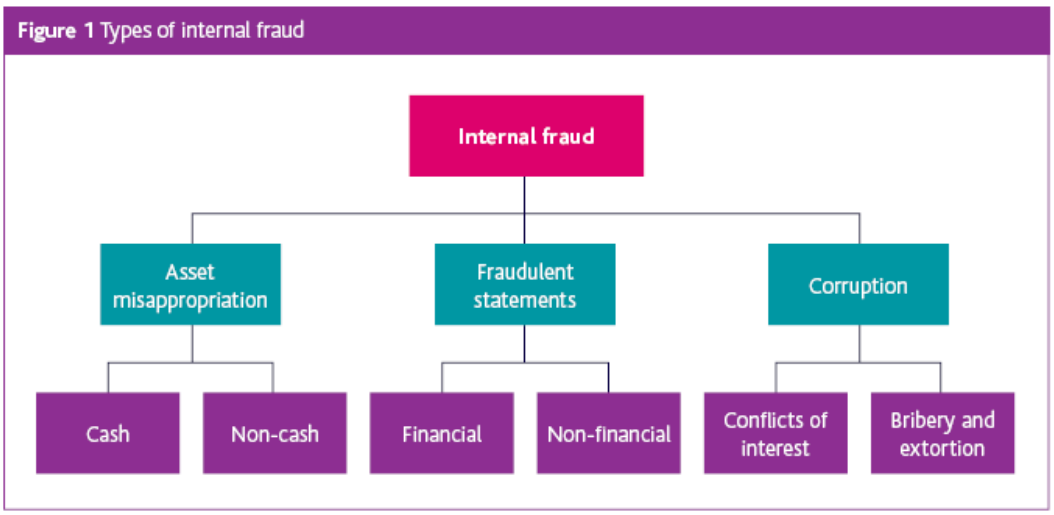
The topic gateway is based on CIMA's publication *Fraud Risk Management: a guide to good practice*, which explores fraud risk management in greater depth.

Application

Internal fraud

There are three main categories of internal fraud that affect organisations. These are summarised in the following diagram.

Figure 1 Types of internal fraud



Adapted from page 8 of *Fraud Risk Management: a guide to good practice*

Further information on common types of internal fraud and methods of perpetration is included in CIMA's *Fraud Risk Management: a guide to good practice*.

Which businesses are affected?

Fraud is an issue that all organisations may face regardless of size, industry or country. If the organisation has valuable property, for example, cash, goods, information or services, then fraud is likely to be attempted.

The scale of the problem

There have been many attempts to measure the extent of fraud, but it is not easy to compile reliable statistics. One of the key aspects of fraud is deception, so fraud can be difficult to identify. Often survey results reflect only the instances of fraud that have actually been discovered. It is estimated that the majority of frauds go undetected. Some frauds may not be reported even when they are found. It is also often hard to distinguish fraud from carelessness and poor record keeping.

Although survey results and research may not give a complete picture, statistics indicate the extent of the problem. There is no doubt that fraud is prevalent within organisations and remains a serious issue. Some surveys put the proportion of companies suffering from fraud as high as 85%. Research shows that fraud is growing, with reported cases of fraud being much higher in 2008 than in 2007. Fraud is likely to continue to grow during economic difficulties.

Organisations may need to keep a particularly close eye on their budgets during a recession, but organisations should see a return on their investment in fighting fraud. Surveys show that UK companies suffered average fraud losses of

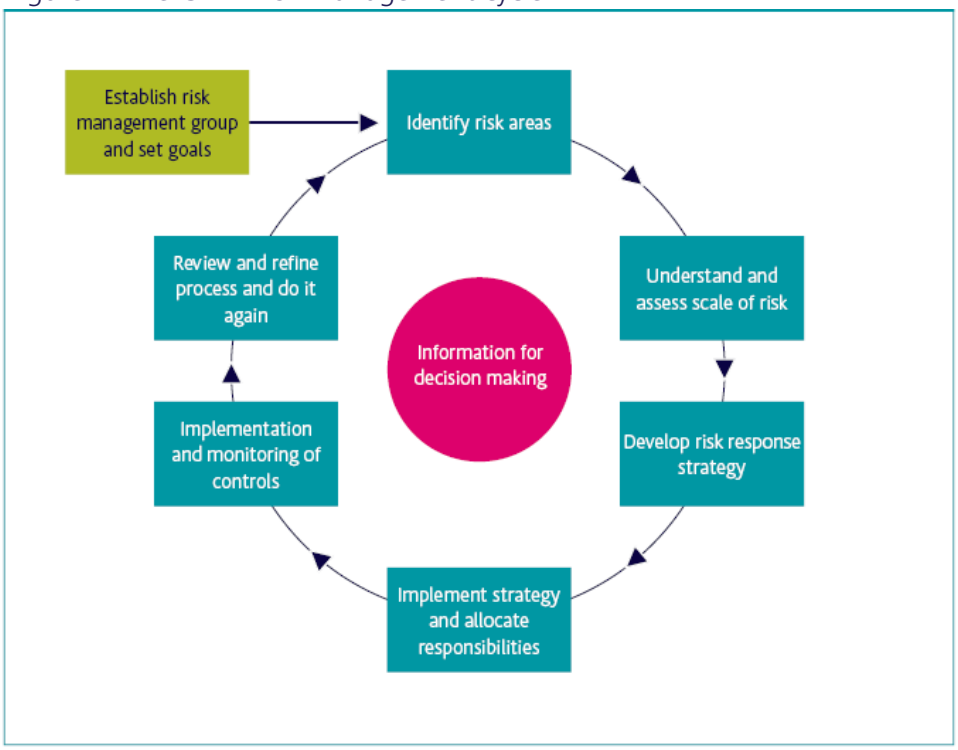
£1.75 million over a two year period. These figures exclude undetected losses and indirect costs to the business such as management costs or damaged reputation. Other research estimates that organisations lose as much as 7% of their annual revenues to fraud.

Given the prevalence of fraud and the negative consequences, there is a compelling argument that organisations should invest time and resources in tackling fraud.

Fraud risk management

In order to manage the risk of fraud, organisations should periodically identify the risks of fraud within their organisation, using the process set out in the CIMA risk management cycle. The CIMA risk management cycle is an interactive process of identifying risks, assessing their impact, and prioritising actions to control and reduce risks.

Figure 2: The CIMA risk management cycle



Adapted from page 19 of *Fraud Risk Management: a guide to good practice*

Fraud risks should be identified for all areas and processes of the business and then be assessed in terms of impact and likelihood. As well as the monetary impact, the assessment should consider non-financial factors such as reputation. Once the scale of risk has been assessed and understood, an organisation should implement an effective anti-fraud strategy for responding to fraud risks.

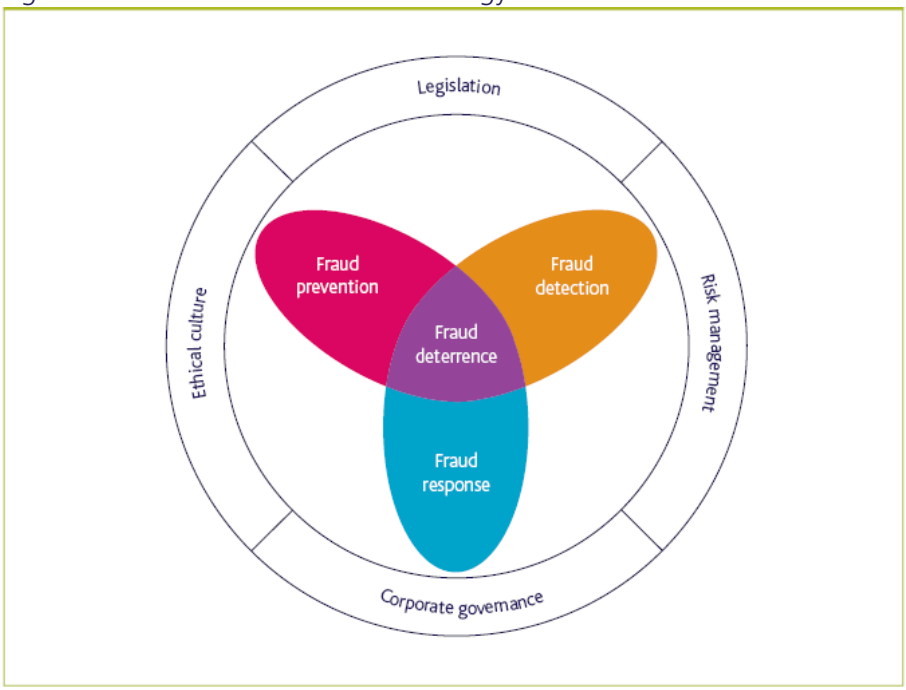
An anti-fraud strategy

An effective anti-fraud strategy has four main components:

- prevention
- detection
- deterrence
- response.

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

Figure 3: An effective anti-fraud strategy



Adapted from page 25 of *Fraud Risk Management: a guide to good practice*

The training received by management accountants is a very good basis for implementing an anti-fraud strategy. Management accountants are expected to have a broad understanding of business processes. They also understand the systems and procedures that an efficient and effective organisation should have. A further asset is the ability to think and act logically, which is something the management accountant develops with experience.

The various components of an effective anti-fraud strategy are discussed in detail in CIMA's *Fraud Risk Management: a guide to good practice*. Some key points are summarised below. These anti-fraud approaches are generic and can be applied flexibly to different organisations and particular circumstances.

Fraud prevention

There are two main elements to fraud prevention:

1. A sound ethical culture.
2. Sound internal control systems.

Developing a sound ethical culture

In order to establish a sound ethical culture, CIMA recommends that organisations have:

1. A mission statement that refers to 'quality' or 'ethics' and defines how the organisation wants to be regarded externally.
2. Clear policy statements on business ethics and anti-fraud, with explanations about acceptable behaviour in risk-prone circumstances.
3. Management which is seen to be committed through its actions.
4. Fraud risk training and awareness for all employees and key business partners.
5. A process of reminders about ethical and fraud policies, for example, an annual letter and/or declarations.
6. Periodic assessment of fraud risk.
7. A route through which suspected fraud can be reported.
8. An aggressive audit process which concentrates on fraud risk areas.

Sound internal control systems

An internal control system comprises all those policies and procedures that collectively support an organisation's operation. Internal controls typically deal with approval and authorisation processes, access restrictions, transaction controls, account reconciliations and physical security. These procedures often include the division of responsibilities, and checks and balances to reduce risk.

The number and type of internal controls that an organisation can introduce depends on its nature and size. Although fraud is prevalent across organisations of all sizes, sectors and locations, research shows that certain business models have greater levels of fraud risk than others. The control environment should be adjusted to fit with the degree of risk exposure. Where possible, internal controls should address warning signs and alerts to minimise fraud.

Fraud detection

It will never be possible to eliminate all fraud. No system is completely 'fraud proof' because many fraudsters can by pass the control systems put in place to stop them. However, if an organisation pays greater attention to the most common indicators, this can provide early warning that something is wrong and increase the likelihood of discovering the fraudster.

Fraud indicators fall into two categories:

1. Warning signs
2. Fraud alerts

Warning signs

Warning signs have been described as organisational indicators of fraud risk. Some examples are given below, categorised under the headings of business risk, financial risk, environmental risk and IT and data risk.

Business risk

Business risk can be indicated by the absence of an anti-fraud policy and culture, together with lack of staff management supervision. Bonus schemes linked to ambitious targets or directly to financial results can point to risky behaviour. Unusual staff behaviour patterns, for example, employees who do not take their annual leave allocation or who are unwilling to share duties, can also indicate business risk.

Other warning signs include:

- inadequate recruitment processes and no screening
- lack of job segregation
- no independent checking of key transactions
- inadequate access controls to physical assets and IT security systems
- poor internal control documentation
- large cash transactions.

Financial risk

Significant pressures on management to obtain additional finance can indicate a financial risk. Other signs include the extensive use of tax havens without clear business justification, along with complex transactions or financial products.

Environmental risk

This can occur when new accounting or other regulatory requirements are introduced. Highly competitive market conditions and decreasing profitability levels can also lead to environmental risk, as can significant changes in customer demand.

IT and data risk

Unauthorised access to systems gives rise to IT and data risk, as do rapid changes in information technology. Users sharing or displaying passwords is also highly risky.

Fraud alerts

Fraud alerts have been described as specific events, or red flags, which may indicate fraud. Some examples of fraud red flags are:

- discrepancy between earnings and lifestyle
- photocopied documents in place of originals
- missing approvals or authorisation signatures
- extensive use of ‘suspense’ accounts
- inappropriate or unusual journal entries
- above average number of failed login attempts.

Fraud detection tools and techniques

Available tools and techniques for identifying possible fraudulent activity include:

- ongoing risk assessment
- trend analysis
- data matching
- exception reporting
- internal audit
- reporting mechanisms.

Fraud response

An organisation's approach to dealing with fraud should be clearly described in its fraud policy and fraud response plan. The plan is intended to provide procedures which allow for evidence gathering and collation. In summary, a fraud response plan should include information under the following headings:

- purpose of the fraud response plan
- corporate policy
- definition of fraud
- roles and responsibilities
- the response
- the investigation
- organisation's objectives with respect to dealing with fraud
- follow up action.

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. Organisations should be clear about how to enforce the rules or controls which are in place to counter fraud risks. They must also ensure that employees know how to report suspicious behaviour.

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

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

There are lessons to be learned from every identified fraud incident. The organisation's willingness to learn from experience is as important as any other response. Organisations should examine the circumstances and conditions which allowed the fraud to occur, with a view to improving systems and procedures so that similar frauds do not occur in future.

Fraud deterrence

It is clear from the diagram in Figure 2 that the various elements of an effective anti-fraud strategy are closely interlinked. Each plays a significant role in combating fraud, with fraud deterrence at the centre. Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organisation is actively fighting fraud and that procedures are in place to identify any illegal activity. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud. There should also be complementary detection to counter the fact that the prevention controls may be insufficient in some cases.

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