MODULE 1 – FUNDAMENTALS OF FRAUDS

Definition of fraud

The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery, and extortion. The legal definition varies from country to country, and it is only since the introduction of the Fraud Act in 2006, that there has been a legal definition of fraud in England and Wales. Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another. Although definitions vary, most are based around these general themes.

Fraud and the law

Before the Fraud Act came into force, related offences were scattered about in many areas of the law. The Theft Acts of 1968 and 1978 created offences of false accounting, and obtaining goods, money and services by deception, and the Companies Act 1985 included the offence of fraudulent trading. This remains part of the Companies Act 2006. There are also offences of fraud under income tax and value-added tax legislation, insolvency legislation, and the common law offence of conspiracy to defraud. The Fraud Act is not the only new piece of legislation. Over the last few years there have been many changes to the legal system with regard to fraud, both in the UK and internationally. This guide focuses mainly on UK requirements, but touches on international requirements that impact UK organisations. In the UK, the Companies Act and the Public Interest Disclosure Act (PIDA) have been amended and legislation such as the Serious Crimes Act 2007 and the Proceeds of Crime Act 2002 (POCA) have been introduced. Internationally the Sarbanes-Oxley Act 2002 (Sarbox) has been introduced in the United States (US), a major piece of legislation that affects not only companies in the US but also those in the UK and others based all over the globe. As well as updating the legislation in the UK, there have been, and will continue to be, significant developments in the national approach to combating fraud, particularly as we see implementation of actions resulting from the national Fraud Review. Appendix 1 gives further information on the Fraud Review. There are also many law enforcement agencies involved in the fight against fraud in the UK, including the Serious Fraud Office, the Serious Organised Crime Agency (SOCA), the Financial Services Authority (FSA), and Economic Crime Units within the police force.

Different types of fraud

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

• crimes by individuals against consumers, clients or other business people, e.g. misrepresentation of the quality of goods; pyramid trading schemes

• employee fraud against employers, e.g. payroll fraud; falsifying expense claims; thefts of cash, assets or intellectual property (IP); false accounting

• crimes by businesses against investors, consumers and employees, e.g. fi nancial statement fraud; selling counterfeit goods as genuine ones; not paying over tax or National Insurance contributions paid by staff

• crimes against fi nancial institutions, e.g. using lost and stolen credit cards; cheque frauds; fraudulent insurance claims

• crimes by individuals or businesses against government, e.g. grant fraud; social security benefi t claim frauds; tax evasion

• crimes by professional criminals against major organisations, e.g. major counterfeiting rings; mortgage frauds; 'advance fee' frauds; corporate identity fraud; money laundering

• e-crime by people using computers and technology to commit crimes, e.g. phishing; spamming; copyright crimes; hacking; social engineering frauds.

According to the Association of Certified Fraud Examiners (ACFE), there are three main categories of fraud that affect organisations. The first of these is asset misappropriations, which involves the theft or misuse of an organisation's assets. Examples include theft of plant, inventory or cash, false invoicing, accounts receivable fraud, and payroll fraud. The second category of fraud is fraudulent statements. This is usually in the form of falsification of financial statements in order to obtain some form of improper benefit. It also includes falsifying documents such as employee credentials. The final of the three fraud categories is corruption. This includes activities such as the use of bribes or acceptance of 'kickbacks', improper use of confidential information, conflicts of interest and collusive tendering. These types of internal fraud are summarised in Figure 1. Surveys have shown that asset misappropriation is the most widely reported type of fraud in UK, although corruption and bribery are growing the most rapidly.

What is risk management?

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

Risk Management Cycle

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

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

Establish a risk management group and set goals

A risk management group should be established whose task it is to facilitate and co-ordinate the overall risk management process. Possible members of the group could include a chief risk officer, a non-executive director, finance director, internal auditor, heads of planning and sales, treasurer and operational staff.

Depending on the size and nature of the organisation, the risk management group may be in the form of a committee who meet from time to time.

The risk management group will promote the understanding and assessment of risk and facilitate the development of a strategy for dealing with the risks identified. They may also be responsible for conducting reviews of systems and procedures to identify and assess risks faced by the business, which include the risk of fraud, and introducing the controls that are best

suited to the business unit. However, line managers and their staff may also be involved in the risk identification and assessment process, with the risk management group providing guidance.

Identify risk areas

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

The techniques of analysis include:

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

Understand and assess the scale of risk

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

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

Develop a risk response strategy

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

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

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

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

Implement the strategy and allocate responsibilities

The chosen strategy should be allocated and communicated to those responsible for implementation. For the

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

Implement and monitor suggested controls

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

Review and refine and do it again

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

Information for decision making

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

Conclusion

There are risks in most situations. Risk management is an important element of corporate governance and every organisation should review their risk status and develop their approach