



POSITION PAPER

THE INTERNAL AUDITOR'S ROLE

IN

THE PREVENTION OF FRAUD

October 1999

Fraud is a Business Risk

Without the active involvement of the internal audit process, it is difficult to see how the board of directors, or equivalent body, can gather sufficient objective information to carry out its stewardship function, be aware of the risks of fraud or report effectively on internal control.

Contents

Executive Summary	Page 3
Introduction	Page 4 - 5
Assessment of Fraud as a Business Risk	Page 6 – 8
The Role of the Board, Management and the Audit Committee	Page 9 – 11
The Role of the Internal Auditor	Page 12 – 13
Reporting Fraudulent Activity	Page 14 – 15
Appendix A Business Ethics And Fraud (a specimen policy)	Page 16
Appendix B Whistleblowing (a specimen policy)	Page 17
Appendix C Comments on ISA 240	Page 18
Acknowledgements	Page 19

1. Executive Summary

- 1.1 Fraud can occur in any organisation, in any sector of economic activity and the perpetrators may be found at all levels of the organisational structure. Fraud is no respecter of national or cultural boundaries.
- 1.2 ECIIA promotes the recognition of fraud as one of many business risks. The possibility of fraud arising – and the extent of its impact – should be part of the periodic corporate risk assessment process undertaken by the board when it reviews its strategies. Internal auditors have a major role to play in this process in providing stakeholders with assurance that this high level process is undertaken with sufficient regularity and the right degree of robustness.
- 1.3 There are no guarantees that any system of control or any group of professional advisors will extinguish the occurrence of fraud. However, the best chance to discourage even the most determined fraudster is to set a high moral “tone from the top”, implement rigorous codes of practice and review all control processes for efficacy.
- 1.4 Directors, managers and all employees should be trained in fraud awareness. Internal auditors should receive wider training in fraud prevention and detection and be required to maintain an up to date knowledge base of this discipline.
- 1.5 The information available to the board, the audit committee and senior management in respect of all internal control operations – and particularly those controls designed to prevent fraud – will be enhanced where an internal auditing function is in place, properly resourced and reporting at a high level.
- 1.6 Internal auditing can make a significant contribution to fraud prevention by undertaking its primary role of providing management with (1) opinions on internal control effectiveness (2) recommendations for control improvement and (3) information on leading-edge techniques for fraud detection and risk assessment.
- 1.7 Internal auditing can provide the organisation with a secure environment for employees to raise concerns when it is perceived that these concerns are not being addressed by line managers. A confidential process, based on best practice, can be put in place by internal auditors which can formally “leapfrog” the hierarchical structure and directly inform the board and its audit committee.
- 1.8 Internal auditing can bring its skills of investigation, analysis and evidence gathering to those circumstances where fraud is suspected. Operating under a board-approved Charter, internal audit can investigate and secure evidence to the point where a report can be made to external authorities – if that is appropriate – with a reasonable chance of a subsequent successful prosecution.

2. Introduction

2.1 What is fraud? Many European countries do not have a legal definition of fraud. The laws invoked to obtain a prosecution usually rely on other specified offences having been committed. These could include conspiracy, theft and forgery. But a fraud cannot occur without *deception*, which usually implies concealment; fraud is, therefore, a pre-meditated act and does not come about because of an omission or an error. A fraud may, of course, begin as a result of an innocent error or mistake not being identified and subsequently being taken advantage of by a fraudster.

Laws in different countries approach the criminal aspects of fraud and the standards of evidence required to prosecute a fraud in various ways. Typically, however, the types of offences under which a fraud may be committed include:

- Conspiracy to cheat and defraud.
- Theft.
- Fraudulent trading.
- Corruption.
- Forgery.
- Insider dealing.
- Conspiracy.

The principles of evidence gathering have a great deal of commonality throughout Europe and are based upon *testimony*, *physical being (real evidence)*, *documentary evidence* and *circumstantial evidence*.

2.1 Fraud can occur in any sector of economic activity or any type of industry and can be committed for the benefit of the organisation or the individual.

Organisational fraud generally takes the form of exploitation of unfair or dishonest advantages that may also deceive an external party. There may also be attempts to mislead potential trade buyers, customers or shareholders by issuing manipulated or misleading market and trade information. Some examples of organisational fraud are:

- Sale or assignment of fictitious or misrepresented assets.
- Improper payments such as illegal political contributions, bribes, kickbacks, and payoffs to government officials, intermediaries of government officials, customers, or suppliers.
- Intentional, improper representation or valuation of transactions, assets, liabilities or income.
- Intentional, improper transfer pricing (e.g. valuation of goods exchanged between related entities). By purposely structuring pricing techniques improperly, management can improve the operating results of an organisation involved in the transaction to the detriment of the other organisation.
- Intentional, improper related party transactions in which one party receives some benefit not obtainable in an arm's-length transaction.
- Intentional failure to record or disclose significant information to improve the financial picture of the organisation to outside parties.
- Prohibited business activities such as those, which violate government statutes, rules, regulations or contracts.
- Underpayment or avoidance of tax.

At the other end of the scale, fraud can be perpetrated for the direct or indirect benefit of an employee, outside individual, or another firm. This may also be to the detriment of another organisation.

Some examples are:

- Acceptance of bribes or kickbacks.
- Account manipulation and management override in order to cover losses and maintain income and bonuses.
- Diversion to an employee or outsider of a potentially profitable transaction that would normally generate profits for the organisation.
- Embezzlement, as typified by the misappropriation of money or property, and falsification of financial records to cover up the act, thus making detection difficult.
- Intentional concealment or misrepresentation of events or data.
- Claims submitted for services or goods not actually provided to the organisation.

2.3 Global increases in criminal activity, particularly that which is drug related, have led to money laundering fears in banks, financial institutions and most European financial centres. By its very nature fraud is a clandestine operation. Perpetrators of frauds do not advertise their activities or their methods. There is also the perception that fraud is a 'victimless' crime; organisations can "well afford the losses".

The extent of fraudulent activity worldwide is unknown but is perceived to be on the increase. In Europe alone, the resignation *en bloc* of European Commissioners in early 1999 following allegations of mis-management of funds, cronyism and conflicts of interest, raised public awareness at a stroke to the extent and level of possible fraudulent activity. At the other extreme, the widespread exposure of the decline and fall of Barings bank at the hands of one rogue trader, crystallised for many people the seemingly unimaginable; that, despite a long and solid history, external regulation and acceptance of governance principles, undetected fraudulent activity can bring down even the most solid-seeming of edifices.

Unfortunately, these are not isolated instances and it is to be expected that, despite the activities of various national committees in Europe (Turnbull in the UK, Vienot in France) and the setting-up of independent regulatory authorities in some countries, Europe will continue to experience significant fraudulent activity. The role of internal audit needs to be reviewed to reflect this challenge. Indeed, there has never been a better time to capitalise on the ability of internal auditing to deliver its primary role of providing assurance to the board and management that all operational risks, including the risk of fraud, have been assessed and are being adequately managed.

It is the ECIIA position that:

- **In the context of fraud, the primary responsibility for internal auditing is to ensure that management has reviewed its risk exposures and identified the possibility of fraud as a business risk, where appropriate.**
- **Auditors need a clearly defined set of responsibilities for the prevention, detection and reporting of fraud.**
- **Awareness measures such as an anti-fraud policy and employee fraud awareness training need to be put in hand to raise the profile of fraudulent activity, its prevention, detection and reporting. This will ensure that auditors *and* organisations enlist the help of customers, employees, shareholders and stakeholders in fighting fraud at all levels.**

3. Assessment of fraud as a business risk

3.1 Internal auditors approach their work from a perspective of risk assessment, looking essentially at high level organisational risks, operational systems risks and control failure risks. The use of risk indices is common practice in, for example, treasury management. Similar indices can be developed and used to forecast potential areas for fraudulent activity. Unusual supplier activity, cartel tendering and employee lifestyles are just a few examples which could form the basis for a weighted index identifying the need for enquiries before a fraud becomes so large or so widespread that corporate damage on a grand scale becomes inevitable.

A series of high profile corporate collapses – most of which have involved fraud - de-layering and business process re-engineering - have all contributed to the increase in corporate exposure to risk and have led to risk being placed close to the top of the agenda for boards, management, internal and external auditors. Nonetheless, risk must not be seen only as a hazard. Risk is also an opportunity and taking risks, albeit calculated ones, part of business, commercial and organisational culture. As the entrepreneur well knows – *no risk, no gain*.

Risk is defined in the IIA *Professional Standards* as

“The probability that an event or action may adversely affect the organisation”(Standard 410.01.1 b)

However, the real nature of risk can be categorised in two ways: **objective or subjective**.

Objective risk has four key components:

- Some potential hazard or threat.
- The likelihood of unwanted conditions or events occurring.
- The consequences or impact of such an occurrence.
- The risk exposure – a function of the likelihood of occurrence and its potential impact i.e. impact multiplied by likelihood.

Risks are thus readily quantifiable so long as monetary values can be assigned to the likelihood of unwanted conditions or events.

A wide range of psychological, cultural and social factors shapes people's perception of risk. This is also known as subjective risk. Such factors include:

- Control: self imposed or externally imposed.
- Dread or scale of impact.
- Familiarity.
- Timing – long term risk is minimised.
- Societal factors e.g. pressure group emphasis.
- Trust.

3.2 All risk assessments are, in practice, a mixture of science, values and judgement and, whilst most observers accept that some risks or hazards should never be accepted, in other cases it is a matter of ensuring that the risk is minimised by the counter measures employed. Management of risk can be compared to financial management and control: it can be used proactively to drive down risks by attempting to anticipate what may go wrong and actively seek to minimise either its likelihood or its impact.

Management of risk needs to be practised throughout the organisation. Different kinds of risks, as well as varying degrees and levels of risk, present themselves at various levels of the

organisation. The corporate level is primarily concerned with the strategic issues of where the business is going and how this vision can be achieved. The commercial level is concerned with transforming the strategy into tactical plans for action. Project management implements the tactical plans through development activities whilst operational management aims to achieve plans by running services and systems to fulfil delivery of products or services.

3.3 At each organisational level, the impact of business risks varies dependent upon the focus of the functions and processes concerned. These can be measured in terms of one or more of the following factors:

- Cost.
- Timeliness.
- Quality.
- Safety (including health).
- Confidentiality (including commercial sensitivity).
- Environmental impact.
- Image.

The possibility of fraud occurring at any or all organisational levels is a risk which has to be recognised by the managers concerned and should be inherent in the management of the so called “risk cycle” to which there are two key aspects:

- Correctly identifying the most important risks; and
- Ensuring that there are strategies in place to manage them.

The analysis of risks and their management are inherently inter-related. The analysis includes:

- Establishing the context and setting perspective.
- Identifying and documenting risks.
- Assessing, quantifying and classifying risks.
- Risk evaluation and modelling.
- Developing risk mitigation and control strategies.
- Obtaining resources and assigning responsibilities.
- Reducing, off-setting or laying-off the risk.
- Risk monitoring and review.

It is the ECIIA position that:

- **fraud, as one of an organisation’s assessed risks, needs to be focused on initially at the highest organisational level i.e. during the board’s strategic review.**
- **the danger of fraud at the strategic level may not be perceived immediately as a risk to the continuing existence of the business, although there are well documented cases where the company has no longer been a going concern as a result of fraud. At the operational level there may be areas where the impact of fraud could be significant, either singularly or collectively. *Risk assessment and identification must, therefore, involve managers at all levels in the organisation.***

ECIIA strongly recommends that all directors and managers receive training in fraud awareness and, where appropriate, risk identification, assessment and evaluation.

3.4 There is an important role for internal audit here:

- Internal audit's accepted role is to provide “an independent appraisal” of the adequacy, application and effectiveness of internal control arrangements put into place by

management. **Internal audit should do exactly this in respect of the strategic assessment of fraud as a business risk by reviewing the process undertaken by the board and management.**

- Internal audit should add value to all the organisation's operations by facilitating the identification and assessment of risks at all levels. It should do this by reviewing the corporate framework for effective risk management processes and ensuring that there are clear, coherent risk policies and standards. **Internal audit should ensure that there are suitable forums for discussing risks at all levels, the clearly defined allocation of responsibility for risk identification and assessment, and finally that there are suitable arrangements in place for management monitor and review.**
- Internal audit provides a regular, objective assurance – particularly where risks may be judged to be critical. *Internal audit must be seen to be a main player in the overall process of managing risk.*

Fraud is a business risk. Its potential needs to be assessed along with all other risks that may impact the survival of the organisation. By ensuring that internal audit, as part of its normal work programme, reviews and reports upon the risk assessment process at all levels of the organisation, the board can both realise the potential of internal auditing and gain a valuable insight into the effectiveness of its own processes.

4. The Role of the Board, Management and the Audit Committee

4.1 Evolution of corporate governance principles in Europe and throughout the world emphasises the close relationship between internal control, effective governance and the *going concern* concept. Put another way, failures of internal control have almost always been identified as a main contributing factor to the many catastrophic business failures that have characterised the final decades of the twentieth century. Control culture, a main pillar of the COSO matrix, (*The Committee of Sponsoring Organisations of the Treadway Commission: Internal Control – Integrated Framework USA 1992*), emanates from the very highest levels of the organisation. Often termed “tone at the top” this culture cascades downwards and is epitomised by the way employees practice their individual occupations. Inappropriate, doubtful or even criminal activity undertaken at board level will, thus, be inevitably reflected throughout the organisation.

The so-called “soft control” approach emphasising codes, culture and peer example depends, also, on the example set from the top. Here, however, there is more reliance on individual responsibility at all organisational levels for ethical and socially acceptable behaviour, not just the performance in the board room. (*CoCo –Criteria of Control Board – Canadian Institute of Chartered Accountants, 1995*)

A recent survey released through AICPA (April 1999, COSO fraud review 1987 –1997) showed that false representation of financial statements was the most significant global fraudulent activity. Since this could only occur with the active connivance of very senior people in any organisation, clearly openness, accountability and integrity – the hallmarks of good governance – remain very much in jeopardy. Fraudulent activity at this level is difficult to detect or even prevent in the face of strong and determined directors or owners.

A 1998 global survey by accountants Ernst and Young *Fraud: The Unmanaged Risk* found that in-house employees perpetrated 84% of serious fraud. Whilst much of this fraudulent activity would have been undertaken with deceit as an intention, it is equally likely that some was caused by individuals noting that certain errors went undetected by the system and could be capitalised upon.

4.2 There are three main issues to be addressed here:

- The extent to which internal control systems can prevent, deter and/or subsequently detect the determined employee fraudster.
- The extent to which more rigorous governance and control requirements – internal and external – will prevent high level fraud.
- The extent to which internal audit can report to the Audit Committee, by virtue of its Charter, on management malpractice.

Changes in company reporting requirements have been a feature of corporate governance reports throughout Europe in recent years. The exposure draft of the 1999 Turnbull Report in the UK (*Internal Control - Guidance for Directors of Listed Companies Incorporated in the UK*) proposes an annual report on internal control and not just financial control. This emphasis accords with earlier UK reports from Cadbury (1992) onwards to Hampel (1998 although Hampel was ambivalent about anything other than financial control) and the UK Combined Code, 1999.

It is also notable that the Fraud Advisory Panel of the UK's Institute of Chartered Accountants of England and Wales (ICAEW) is debating the need to extend the sort of disclosures recommended by Turnbull. In other words a similar statement to that on internal controls could be insisted upon in the annual report and accounts. This would require directors to disclose, for example, details of systems that were in place to combat and detect fraud.

Similar requirements in respect of commenting on internal control exist in Luxembourg for relevant financial and credit institutions (*IML Circular 98/143*), in Holland as a result of the report on the Committee on Corporate Governance and in France where, following the Vienot Report, regulations were strengthened in credit institutions and require such institutions to make an annual report “on the conditions in which internal control is conducted”. The difficulty with these reporting requirements, admirable as they are, is that they are susceptible to being just another piece of “window dressing” that remains subject to the manipulation of high level employees. In the UK, this point was hammered home by the ICAEW Fraud Advisory Panel in their first annual report (1999) which indicated that, yet again, most fraud is perpetrated by senior management.

4.3 One of the ways in which the Board can address fraud corruption and other malpractice is through the publication of a policy statement relating to business ethics and fraud prevention. The aim of the policy should be to set the tone of acceptable behaviour, define expectations and provide a yardstick against which employees can assess their actions. It should be approved at the top level of the organisation and promulgated to all management and staff. An outline of issues to consider can be found at Appendix B.

The fundamental message which has to be given is that employees work under a set of rules, which everyone in the company from top management down must accept. Those who break these rules, including those who commit fraud, are not only committing possible criminal acts but are actively working against corporate goals and to the detriment of shareholder value.

The essential corollary to the code of conduct, *in the view of ECIIA*, is a rigorous internal audit process that can provide a comfort factor for stakeholders by virtue of its diligence. Requiring only the statutory auditor to audit the process by which the board provides its statement on internal control and then report, internally, to the board at large, may not be perceived by the public as a process that is either sufficiently open or sufficiently rigorous. Even this process, however, could be enhanced were there to be explicit reference to the work of internal audit in this area by the statutory auditor.

4.4 International Standard for Auditing (ISA) 240 establishes standards and provides guidance on the statutory auditor’s responsibility to consider fraud and error in an audit of financial statements. **ECIIA believes that the current review of this ISA being undertaken by the International Auditing Practices Committee would benefit from an explicit requirement for the statutory auditor to consider the work of the internal auditor and to discuss any significant findings with him. There are other areas where ECIIA believes that its input to a new ISA on this matter could significantly affect its value to statutory auditors and managements alike. Specific comments are in Appendix C.**

4.5 In its October, 1996 response to the European Commission’s Green Paper *The Role the Position and the Liability of the Statutory Auditor in the European Union (July 1996)*, ECIIA stated *inter alia*:

“Establishing, running and maintaining an effective system of internal control calls for skills which most managers do not possess”.

This was said in the context of the debate at that time concerning the so-called “expectations gap” between what was delivered by statutory auditors and the public’s perception of the product delivered. Thus, a statutory auditor’s “clean” report was perceived by stakeholders as a “seal of approval” covering legal compliance, absence of fraud and going concern status, as well as covering environmental and social obligations. In other words, that internal control,

as established by management in order to achieve their objectives, had been, is and would be completely effective.

Whilst much has changed in the field of voluntary and mandatory compliance and regulation for aspects of corporate governance – which includes action against fraud – internal control has remained central to the debate. Internal control is an integral part of the management process. It is derived from the way in which directors and managers run their businesses. The COSO report defines internal control as, “...a process effected by the board of directors, managers and other personnel, designed to provide reasonable assurance regarding the achievement of objectives” in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

In terms of COSO, all organisations encounter risk exposure from both internal and external sources. These exposures can affect their ability to survive as a going concern, compete successfully, maintain their financial strength and maintain the quality of both products and services and staff. Clearly, fraud is a major risk exposure in this respect and could affect the current and future viability of the organisation.

The annual programme of work undertaken by internal audit is geared to the risks to which the organisation is exposed and to the risks identified in each process or system to be audited. The outcome of internal auditing activity should be:

- An opinion on the effectiveness of internal control given by the Head of Internal Audit to the audit committee.
- A better assessment of the state of internal control by the audit committee as a result of the continuous interaction throughout the year between internal audit and the audit committee.

It is the ECIIA position that:

Without the active involvement of the internal audit process, it is difficult to see how the board can gather sufficient objective information to carry out its stewardship function, be aware of the risks of fraud or report effectively on internal control.

4.5 ECIIA believes strongly that management retains the responsibility for putting in place an appropriate control structure designed to ensure achievement of organisational objectives. The control structure should *inter alia* ensure mitigation of business risks, including risk of fraud and be reviewed for efficacy from time to time. ECIIA also believes that a properly constituted Audit Committee has a pivotal role to play in these matters but that, without the necessary awareness training, it will be unable to fulfil its overview of the processes and risks involved.

The role of internal audit is to advise and assist management in ensuring that control is effective by devising a risk based programme of work which covers the organisation’s main operations and systems. Internal audit should also ensure that the board and senior management have provided themselves with suitable training opportunities in order to understand the complexities of risk management, internal control and fraudulent activity.

5. The Role of the Internal Auditor

5.1 What can internal audit contribute to the prevention and detection of fraud? It is the responsibility of management to put in place systems and processes that will prevent and detect fraud within an organisation. Internal audit can assist them in this task through its:

- Assessment and evaluation of the risk and control strategies of the organisation.
- Involvement in the improvement of risk and control strategies.
- Provision of assurance that the organisation is 'in control' relative to its risks.

First, then, internal audit must review the organisation's:

- Attitude to risk at board level - for example, are board members risk takers, risk averse or somewhere in the middle and how is this attitude disseminated across the organisation.
- Strategies on risk - are the key risks in different areas of the organisation treated differently, for example by transfer, assignment, avoidance or acceptance of risk.
- Overall risk management systems - are these embedded within organisational functions, to reflect and represent the strategies on risk established in specific areas.

5.2 The professional *Standards* of the Institute of Internal Auditors require its members to review the risks associated with the safeguarding of assets (*Standard 330*). This requires them in the course of their work to specifically consider the various types of losses, such as theft, improper or illegal activities. They should assist in the deterrence of fraud by examining the adequacy and the effectiveness of control, commensurate with the extent of exposure/risk in the various segments of the organisation's operations. In carrying out this responsibility internal auditors should determine whether:

- The organisation's environment fosters an awareness of risk and control
- Realistic organisational goals and objectives are set
- Written policies (i.e. codes of conduct) exist that describe prohibited activities and the actions required whenever violations are discovered.
- Appropriate authorisation procedures for transactions are established and maintained.
- Policies, practices, procedures, reports and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas.
- Communication channels provide management with adequate and reliable information.
- Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.

Organisations function in an environment where constant adaptation and improvement are the norm. It is therefore important that management institute processes for continually monitoring, adapting and improving their risk/control strategies, structures and systems. In addition, they require some form of assurance that they are “in control” relative to the risks and the potential for fraud that they may be exposed to.

It is the ECIIA position that:

Internal audit is a key player in the process of risk assessment and evaluation, improvement and assurance through:

- **The implementation of risk based audit plans.**
- **Its involvement in strategic consultancy projects.**
- **Its input to the development of new systems.**
- **Its introduction and implementation of Control and Risk Self Assessment.**

5.3 Internal audit assists management in achieving its objectives but can also aid the audit committee in meeting its responsibilities, particularly in the areas of risk and internal control, fraud and internal investigations. Audit committees should consider whether the internal audit function's role is appropriate, has suitable reporting lines and whether it has adequate resources. A strong internal audit function, reporting to an audit committee which has an interest in enhancing all aspects of business performance, has much to contribute to the maintenance of effective control systems.

'Companies without a strong internal audit function will be unable to provide an audit committee with sufficient information to fulfil its responsibilities'.

(European Commission 1996 Green Paper on Auditing)

5.4 For internal audit to provide an effective assurance service it is necessary that the board and management understand their responsibility to:

- Set the moral climate in which the enterprise functions.
- Provide the structure to accomplish its plans and follow its policies.
- Understand its risk attitude and develop a risk management strategy.
- Establish and maintain internal controls.
- Determine the cost versus control ratios, keeping in mind the equation: exposures minus safeguards equal risks.
- Establish and maintain the lines of communication and systems of reporting within the organisation and for knowing what is going on.

Internal auditors are responsible for determining whether all these actions have been taken and whether they are carried out efficiently and effectively.

The work undertaken by internal audit is geared to the risks to which the organisation is exposed and to the risks identified in each process or system to be audited. The outcome of annual internal auditing activity should be:

- (a) A better understanding within the organisation of how to identify and manage risks that could give rise to fraud or abuse,
- (b) An opinion on the effectiveness of internal control given by the Head of Internal Audit to the Audit Committee and the Board,
- (c) A better assessment on the state of internal control by the Audit Committee as a result of the continuous interaction throughout the year between them and internal audit.

It is the ECIIA position that:

All European listed companies - and other relevant organisations – should have the services of a properly resourced internal auditing function and a professionally qualified Head of Internal Audit who reports at the highest levels of the organisation i.e. board and audit committee. This is the best means available to provide stakeholder assurance that risk assessment and control regimes are in place and are both adequate and effective.

6. Reporting Fraudulent Activity

6.1 Not all internal or external audit work will detect fraud. Nor can the work of other professionals such as Certified Fraud Examiners guarantee detection. Internal auditors do have the advantage, however, of being familiar with the in-house situation. The suspicion or detection of fraudulent activities normally arises through:

- The findings of audit work; or
- Accidental discovery or
- Through concerns being expressed by employees within the company.

All review agencies – and particularly internal audit - when reviewing systems, should ensure that there are adequate controls, and if not, recommend improvements to promote compliance with acceptable procedures and practices. Improvements suggested may include those to prevent, detect or deter fraud. Internal auditors are required by their *Standards* to exercise “due care”, defined as exercising a competent level of skill and care such as could be expected from a comparable professional. Due care does not mean that internal auditors should detect all frauds, but it does require reasonable care and prudence; internal auditors should be alert to errors and irregularities which may be indicators of fraud.

6.2 Concerned employees of an organisation can report suspicions of fraud and abuse. This is popularly known as ‘whistleblowing’. Whistleblowing has been the subject of legislation in the USA, Australia, New Zealand and the UK during the last ten years. An effective system for raising concerns should include:

- A clear statement that malpractice is taken seriously in the organisation and an indication of the sorts of matters regarded as malpractice.
- Respect for confidentiality of staff raising concerns if they wish.
- The opportunity to raise concerns outside the line management structure.
- Penalties for making false and malicious allegations.
- An indication of the proper way in which concerns may be raised outside the organisation if necessary.
-

It is good management practice to ensure that sufficient avenues are specified formally for staff to communicate their concerns internally within the business and that robust procedures are in place to ensure that communicated concerns are thoroughly addressed.

It is the ECIIA position that:

internal audit can be used as a conduit outside the line management process for staff to express their concerns in a confidential environment. It is, however, important that the board indicates clearly how internal audit is expected to handle such matters. Internal audit in turn should strictly follow the approved procedures.

To assist staff in voicing their concerns many organisations have adopted a whistleblowing policy statement. The main features of such a policy are included in Appendix B.

6.3 If, as a result of audit work or staff concerns, fraud is suspected by internal audit, consideration should be given as to the need to advise management of the position. This can be done orally or by written, interim or final report containing the findings and including a conclusion as to whether sufficient information exists to conduct a full investigation. Discussions may take place with the organisation's legal advisors before a written report is prepared.

On the issue of timing, the appropriate level of management should be told as soon as there is reasonable suspicion of fraud. They should also be made immediately aware if it is considered that the fraud materially affects previously published financial statements.

It is important that the internal auditor considers who might or might not have been involved in internal fraud so as to ensure that the issue of a report does not alert them. If those involved are alerted any subsequent prosecution could be put at risk if they have the opportunity to tamper with or destroy evidence. Early warning might also provide the opportunity for them to realise the proceeds of fraud and conceal their whereabouts.

The written report at the end of this phase should include all findings, conclusions, recommendations and corrective action taken. It may also be submitted to the organisation's legal advisors for review.

6.4 An important issue to consider is the circumstances in which, and the timing at which, suspicions or evidence of fraud should be reported to external regulators or the police. Where there is a specialist function within the organisation dealing with fraud, there should be an agreed policy and protocol for so doing, which should involve the organisation's legal advisors.

Where this is not the case and the fraud comes to light as a result of internal audit work, or is investigated by internal audit at the request of management, the organisation's legal advisors should be consulted as soon as there is reasonable suspicion that fraud has been committed.

Failure to properly investigate fraud or to obtain legally valid evidence might jeopardise any subsequent prosecution. If the internal auditor or any other internal investigator is not fully conversant with, or experienced in the rules of evidence it is imperative that the police are advised once there is reasonable suspicion so that this risk can be avoided.

6.5 Fraud investigation is a specialised role. Internal audit can conduct fraud investigations but only if they have the proper expertise and authority. In some organisations there will be specialist teams responsible for fraud investigation either within internal audit or outside of it. Normally internal audit would assist these specialist teams in their investigations.

It is the ECIIA position that:

internal auditors are able to play an important role in fraud investigations because internal auditors:

- **Think objectively and are used to working with facts and objective analyses.**
- **Understand the nature of control and can evaluate its effectiveness. Fraud and abuse occurs where controls are weak and ineffective. The internal auditor should know the systems in place within the organisation and be able to identify the specific weaknesses that have been exploited.**
- **Can institute interrogations of applications files and systems logs to be able to prove what has happened.**
- **Understand evidence or the 'audit trail' and how it can be secured. Internal auditors should know what audit trails exist, in what form they are held, how they are held and what retention period is applicable.**

Appendix A

Business ethics and fraud (specimen policy)

Outline of areas to address

- A policy statement issued by the Chairman of the Board/Chief Executive stressing the organisation's commitment to the highest ethical standards and requiring all employees to make themselves aware of and comply with the policies and guidelines issued on corporate conduct.
- The need for all employees to comply with all laws and regulations applicable to the place of business.
- Guidance on holding other positions, for example, directorships outside the business, and on engaging in personal transactions within the business or which might affect the business - such guidance addressing issues relating to conflicts of interest.
- Where the organisation is a public company, a requirement for employees in possession of share price sensitive information to comply with the codes of practice relating to insider dealing.
- The need for compliance with policies relating to information security and confidentiality
- Policies relating to the payment of inducements, gifts and entertainment and the acceptance of such gifts and entertainment.

Topics to be considered within the policy specifically relating to fraud should include:

- A statement that employees should always act with integrity at all times and should not engage in fraudulent activity of any kind even that which may benefit the company.
- A clear assertion that the policy relates to all members of staff irrespective of seniority or length of service.
- A commitment to ensure that cost-effective controls and procedures will be installed to prevent, detect, deter and deal with fraud.
- A statement that it is the responsibility of each employee to safeguard company assets.
- A statement that all employees should encourage good standards of health and safety in their work environment.
- A requirement that all employees should understand and use the procedures raised in the aforementioned section on 'systems for encouraging and channelling expressions of concern of fraud'.
- A statement that relations with government institutions must not break any guidelines on ethics and integrity.
- A statement that any communication outside of the organisation should be adequate, appropriate and accurate, and is to be made only through the authorised channels of the company.
- The allocation of responsibility for the investigation of suspected fraud or misconduct and the internal reporting procedures which will apply where fraud takes place.
- A requirement for all employees to assist with any investigation when required.
- The policy to be applied in relation to suspension, dismissal and reporting to the police with a view to prosecution (with a provision that if the policy is to report all cases to the police this may be only varied by the express agreement of the Chief Executive or some other member of senior management).
- A commitment to seek financial recovery through civil proceedings.
- The requirement to ensure that all staff are informed of the business conduct and anti-fraud policy as part of their induction procedures and receive a copy of the policy which they have to sign as evidence that they have read it and agree to abide by its contents. A copy should be included in the staff handbook.

Appendix B

Whistleblowing (specimen policy)

Outline of areas to address

- Scope of the statement to cover frauds, corruption and malpractice, criminal or illegal behaviour, miscarriage of justice, damage to health and safety etc.
- The organisation commits generally to the highest standards and specifically to involve staff in the development of its procedures on confidential reporting. It undertakes to monitor the policy, keeping confidential records of all matters raised through the whistleblowing policy and ensuring that an appropriate committee receives reports with an assessment of the effectiveness of the policy and any emerging patterns.
- Encouraging employees to express concerns and suggesting they might like to come forward with a colleague or another person. There should be a promise of support and confidentiality where possible and it should not be described as a disciplinary offence to discourage staff from expressing concerns or victimisation following expression of a concern. There should be a specific commitment to ensuring that expressing concerns will not affect careers.
- Employees are encouraged to 'blow the whistle' within the organisation rather than overlooking a problem or raising the issue outside. Employees are reminded that organisational rules require staff not to disclose confidential, false or misleading information. The policy statement should point out that the public interest disclosure act gives legal protection to whistleblowers who honestly and reasonably believe that the information they disclose or the allegations they make are substantially true.
- A flexible route for communicating concerns should be allowed for. In most cases this will be to the immediate manager. Allowance is however made for the concern to be expressed at the discretion of the concerned person direct to the internal audit service, or to a senior officer or to the central services director or even to the chief executive. Staff, are given the right to ask for a confidential meeting and are reminded that both parties should treat such contacts in confidence.
- It is recognised that there may be exceptional circumstances in which it might be best to contact an external agency.
- Assurance should be provided that all concerns will be looked into carefully and thoroughly and acted upon appropriately. Provision for either internal or independent investigation is made. Fairness to all parties is warranted. If requested the organisation agrees to try and let the concerned person know the results of the investigation and the action proposed.
- The organisation commits to acknowledging a communicated concern within seven days, with an indication of how the organisation proposes to deal with the matter and likely timescale. If a decision is made not to investigate the reasons will be given. The concerned person is assured of as much information as possible on the outcomes of the investigation, subject to certain constraints.

Appendix C

ISA 240

Article 5. Responsibility of Management.

This Article could be enhanced by the addition of comments relating to (1) the use of an effective and professionally qualified internal auditing function and (2) the implementation by the board of a code of business ethics.

Article 7. Risk assessment.

A good relationship between internal and external auditor will help to reduce the possibility of fraud and error. This Article should be amended to ensure that the statutory auditor actively discusses with internal audit the internal auditor's opinion of the risk management process and the effectiveness of internal control systems.

Article 14.

This Article should take cognisance of a code of ethics and an internal "whistleblowing" procedure which would allow the confidential reporting of concerns to internal audit or another review agency, thus avoiding the management over-ride possibility.

Articles 17 and 18.

It is essential that the statutory auditor informs the audit committee when there is any indication, as a result of the auditor's work, that fraud or error may exist.

Articles 21, 22 and 23.

The circumstance surrounding any limitation of fraud or error reporting to users of the auditor's report should be explicitly indicated.

ACKNOWLEDGEMENTS.

ECIIA gratefully acknowledges the work of the co-ordinators for this Position Paper:

Marian Lower, United Kingdom
Neil Cowan, Director General, ECIIA

And the participation of the members of the ECIIA Project Group:

Louis Vaurs, France
Dr Peter Diekman, Netherlands
Carolyn Dittmeier, Italy
Einar Dossland, Norway

ECIIA would also like to thank the Institute of Internal Auditors UK and Ireland for the extensive use made of Professional Briefing Notes 12 and 13: *Fraud and the Internal Auditor* and *Managing Risk*; the UK charity Public Concern at Work for the Whistleblowing policy specimen and the Institute of Internal Auditors Inc for extracts from *The Competency Framework for Internal Auditing*.

ECIIA has previously published the Position Paper *Internal Auditing in Europe* (1996). Membership of ECIIA is open to institutes of internal auditing from countries within the wider economic and geographic area of Europe and the Mediterranean basin. There are currently 28 member bodies.

The European Confederation of Institutes of Internal Auditing

*Meir 24
2000 Antwerp
BELGIUM*

Tel +323 232 17 82
Fax +323 226 68 02

© ECIIA