PRISE DE POSITION

LES CAHIERS DE LA RECHERCHE

Le rôle de l'Auditeur Interne dans la Prévention de la Fraude :

Prise de position de l'ECIIA

Versions anglaise et française

IFACI Institut de l'Audit Interne

Le rôle de l'Auditeur Interne dans la Prévention de la Fraude :

Prise de position de l'ECIIA (Octobre 99) (European Confederation of Institutes of Internal Auditing)

Versions anglaise et française

IFACI Institut de l'Audit Interne

IFACI – Paris – Septembre 2000
ISBN : 2-9515475-1-X

AVANT-PROPOS

Le rôle de l'auditeur interne face au risque de fraude n'est pas toujours clairement perçu par les différentes parties prenantes. Pourtant, les Normes pour la Pratique Professionnelle de l'Audit Interne définissent les diligences requises en cas de détection d'indices de fraude ainsi qu'en matière de prévention, notamment à travers l'évaluation de la pertinence et de l'efficacité du contrôle interne.

L'ECIIA, European Confederation of Institutes of Internal Auditing, (*Confédération Européenne des Instituts d'Audit Interne)* a déposé en octobre 1999 à la Commission Européenne une prise de position sur le sujet, intitulée *The Internal Auditor's Role in the Prevention of Fraud* (" Le Rôle de l'Auditeur Interne dans la Prévention de la Fraude ").

Il nous a semblé important de proposer et de diffuser, à destination des pays francophones, la traduction française de cette prise de position. Celle-ci préconise que la fraude soit reconnue comme un risque inhérent à l'activité de l'entreprise et, à ce titre, insiste sur la contribution majeure que doit apporter l'auditeur interne, soutenu par tous les acteurs de l'entreprise, au processus de prévention et de détection de la fraude.

Cette prise de position nécessitera sans doute des commentaires et des recommandations de mise en œuvre qui pourront faire l'objet d'une publication ultérieure.

REMERCIEMENTS

L'Institut de l'Audit Interne remercie l'ECIIA de l'avoir autorisé à traduire et à diffuser sa prise de position.

L 'Institut de l'Audit Interne remercie également pour le soutien apporté à la traduction française de la prise de position de l'ECIIA :

– Dominique Vincenti, Directeur de l'Audit Interne, Conforama Management Service,

– L'équipe Ernst & Young, sous la responsabilité de Jean Coroller, Associé Business Risk Management.

ERNST & YOUNG

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.

La fraude est un risque de l'entreprise

Sans l'implication active du processus d'audit interne, on imagine mal comment le conseil d'administration, ou tout organe équivalent, peut réunir suffisamment d'informations objectives pour s'acquitter de sa fonction de gérance, avoir conscience des risques de fraude ou rendre compte efficacement des contrôles internes.

CONTENTS

Executive Summary 8
Introduction 10
Assessment of Fraud as a Business Risk 16
The Role of the Board, Management and the Audit Committee 22
The Role of the Internal Auditor 30
Reporting Fraudulent Activity 36
Appendix A Business Ethics And Fraud (a specimen policy) 42
Appendix B Whistleblowing (a specimen policy) 46
Appendix C Comments on ISA 240 50
Acknowledgements 52

TABLE DES MATIÈRES

1. Résumé 9
2. Introduction 11
3. Évaluation de la fraude en tant que risque de l'entreprise 17
4. Le rôle du conseil d'administration, de la direction et du comité d'audit 23
5. Le rôle de l'auditeur interne 31
6. Rendre compte d'une activité frauduleuse 37
Annexe A Ethique des affaires et fraude (modèle de procédure) 43
Annexe B Dénonciation (modèle de procédure) 47
Annexe C ISA 240 - Commentaires 51
Remerciements 53

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.

1. RÉSUMÉ

1.1 La fraude peut survenir dans n'importe quelle organisation et dans n'importe quel secteur d'activité ; les fraudeurs sont susceptibles de se trouver à tous les niveaux de l'entreprise. La fraude n'est pas plus respectueuse des frontières nationales que des frontières culturelles.

1.2 L'ECIIA préconise que la fraude soit reconnue comme l'un des nombreux risques inhérents à l'activité de l'entreprise. Evaluer la probabilité de survenance d'une fraude – et son impact – devrait faire partie du processus périodique d'évaluation du risque dans l'entreprise réalisé par le conseil d'administration dans le cadre de la révision de ses stratégies. L'audit interne a un rôle essentiel à jouer dans ce processus, en assurant aux parties prenantes que ce processus de grande importance est réalisé avec une régularité suffisante et de façon rigoureuse.

1.3 Il n'existe aucune garantie qu'un système de contrôle ou qu'un groupe de professionnels éliminera tout risque de fraude. Cependant, la meilleure chance de décourager le fraudeur le plus déterminé consiste à « donner le ton » en terme d'éthique, depuis le haut de la hiérarchie, à mettre en place des codes de pratique rigoureux et à revoir l'efficacité des procédures de contrôle existantes.

1.4 La Direction, le management et tous les employés devraient être sensibilisés à la fraude. Les auditeurs internes devraient recevoir une formation plus large sur la prévention et la détection de la fraude. Ils devraient être tenus d'actualiser leurs connaissances dans ce domaine.

1.5 Pour que le conseil d'administration, le comité d'audit et la direction disposent d'informations de qualité sur le contrôle interne, en particulier, sur les contrôles concernant la fraude, il est nécessaire de mettre en place une fonction d'audit interne dotée de ressources adéquates et rendant compte à un niveau élevé de la hiérarchie.

1.6 L'audit interne peut contribuer de manière significative à la prévention de la fraude en apportant à la direction, conformément à son objectif premier, (1) une opinion sur l'efficacité du contrôle interne, (2) des recommandations sur l'amélioration des contrôles, et (3) des informations sur les techniques les plus modernes en matière de détection de la fraude et d'évaluation du risque.

1.7 L'audit interne peut offrir à l'entreprise un environnement permettant aux employés de faire entendre leurs préoccupations lorsqu'ils considèrent qu'elles ne sont pas prises en compte par leurs supérieurs hiérarchiques. Une procédure confidentielle, issue des meilleures pratiques, peut être mise en place par les auditeurs internes afin de passer outre la hiérarchie et d'informer directement le conseil d'administration et son comité d'audit.

1.8 L'audit interne peut apporter ses compétences en matière d'investigations, d'analyse et de collecte de preuves dans les cas de suspicion de fraude. L'auditeur interne, qui opère dans le cadre d'une Charte approuvée par le conseil d'administration, peut enquêter et réunir les preuves nécessaires permettant d'adresser, le cas échéant, un rapport aux autorités extérieures avec une probabilité raisonnable de succès dans les poursuites ultérieures.

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*.

2.2 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.

2. INTRODUCTION

2.1 Qu'est-ce que la fraude ? Nombreux sont les pays européens qui n'ont pas de définition légale de la fraude. A défaut, les poursuites engagées s'appuient généralement sur les textes relatifs à l'entente frauduleuse, le vol et les faux et usages de faux. Toutefois, une fraude ne peut intervenir sans *tromperie*, ce qui implique généralement une dissimulation ; la fraude est par conséquent un acte prémédité, et ne résulte pas d'une erreur ou d'une omission. Une fraude peut, bien entendu, trouver son origine dans une erreur innocente et non identifiée, exploitée ultérieurement par un fraudeur.

Les lois des différents pays ont des approches différentes des aspects criminels de la fraude et des niveaux de preuve requis pour engager des poursuites. De façon générale, on peut toutefois classer les délits selon la typologie suivante :

- l'escroquerie
- le vol
- le commerce frauduleux
- la corruption
- le faux et usage de faux
- le délit d'initié
- l'entente frauduleuse

Les principes de collecte de preuves ont beaucoup de points communs dans toute l'Europe : ils reposent sur le *témoignage*, l'*existence physique (preuve matérielle)*, les *preuves documentaires* et les *preuves indirectes*.

2.2 La fraude peut intervenir dans n'importe quels secteur économique et type d'activité. Elle peut être commise pour profiter à l'entreprise ou à un individu.

La fraude dans l'entreprise se traduit généralement par l'exploitation d'avantages inéquitables ou malhonnêtes, susceptibles de tromper une partie extérieure. Il peut aussi y avoir tentative de tromperie d'acheteurs potentiels, de clients ou d'actionnaires par la publication d'informations remaniées ou trompeuses sur le marché et les activités de la société.

Exemples de fraude dans l'entreprise :

- Vente ou cession d'actifs fictifs ou présentés de manière trompeuse.
- Paiements illégaux tels que contributions illégales à des fins politiques, corruption, dessous-de-table à des fonctionnaires du gouvernement, ou leurs représentants, à des clients ou des fournisseurs.
- Présentation ou valorisation incorrecte et délibérée des opérations, de l'actif, du passif ou des revenus.

- 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.

- Prix de cession intentionnellement incorrect (ex. valorisation des marchandises échangées entre des entités liées). En choisissant délibérément un mode de fixation des prix incorrect, la direction peut améliorer les résultats d'exploitation de l'une des entreprises impliquées dans la transaction au détriment de l'autre entité.
- Transactions intentionnellement incorrectes entre parties liées, dans lesquelles une partie bénéficie d'un avantage qu'elle n'aurait pas eu lors d'une opération réalisée dans des conditions normales.
- Défaut intentionnel d'enregistrement ou de divulgation d'informations importantes afin d'améliorer l'image financière de l'entreprise auprès de tiers.
- Activités commerciales interdites, en violation notamment des lois, réglementations ou contrats.
- Paiement partiel de l'impôt ou évasion fiscale.

Par ailleurs, la fraude peut être réalisée au profit direct ou indirect d'un employé, d'une personne extérieure à l'entreprise ou d'une autre société. La fraude peut également être commise au détriment d'une autre entreprise.

Exemples :

- Acceptation de pots de vin ou dessous de table.
- Manipulation des comptes et contournement de la direction pour couvrir des pertes et maintenir le niveau de bénéfice et de primes.
- Détournement vers un employé ou une personne extérieure d'une opération potentiellement rémunératrice qui devrait normalement engendrer des bénéfices pour l'entreprise.
- Détournement de fonds ou de biens et falsification des comptes pour dissimuler cet acte, rendant sa détection plus difficile.
- Dissimulation délibérée ou présentation intentionnellement trompeuse de faits ou de données.
- Réclamations présentées au titre de services ou de marchandises qui n'ont, en réalité, pas été fournis à l'entreprise.

2.3 L'augmentation généralisée de l'activité criminelle, notamment ce qui touche au commerce de la drogue, a entraîné la défiance des banques, des institutions financières et de la plupart des centres financiers européens à l'égard du blanchiment d'argent. Par nature la fraude est une opération clandestine. Ceux qui la commettent ne rendent publiques ni leurs activités ni leurs méthodes. La fraude est également perçue comme un crime « inoffensif », les entreprises pouvant « bien se permettre les pertes occasionnées ».

On ne connaît pas l'étendue des activités frauduleuses au plan mondial, mais il semblerait qu'elles soient en augmentation. Pour ne prendre en exemple que l'Europe, la démission en bloc des Commissaires européens début 1999, à la suite d'allégations de mauvaise gestion de fonds, de népotisme et de conflit d'intérêt, a éveillé l'attention du public sur l'étendue et le niveau des activités frauduleuses possibles. Dans un autre domaine, la large publicité qui a été faite autour de la crise et de la faillite de la banque Barings du seul fait d'un courtier indélicat a illustré ce qui, dans l'esprit de nombreuses personnes, paraissait inimaginable : en dépit d'une histoire longue et stable, de l'existence d'un système de

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.

régulation et de la reconnaissance des principes de gouvernement d'entreprise, un acte frauduleux non décelé a pu entraîner la chute de l'édifice apparemment le plus solide.

Il ne s'agit malheureusement pas de cas isolés, et il faut s'attendre à ce que, en dépit des actions entreprises par différents comités nationaux en Europe (Turnbull au Royaume-Uni, Viénot en France) et la mise en place d'autorités de régulation indépendantes dans certains pays, l'Europe continue à connaître une activité frauduleuse importante. Le rôle de l'audit interne doit être repensé pour prendre en compte le défi qui se présente. En effet, on ne pouvait trouver de meilleur moment pour tirer parti du rôle premier de l'audit interne, qui consiste à assurer aux organes exécutifs et à l'équipe de direction que tous les risques d'exploitation, y compris le risque de fraude, ont été évalués et sont gérés de manière adéquate.

La position de l'ECIIA est la suivante :

Dans un contexte de fraude, la principale responsabilité de l'audit interne est de s'assurer que la direction a examiné son exposition au risque et identifié, lorsque cela se justifie, la possibilité de fraude comme un risque de l'entreprise.

Les responsabilités des auditeurs internes en matière de prévention, détection et information de la fraude doivent être clairement définies.

Des mesures de sensibilisation telles qu'une politique de lutte contre la fraude ou la formation des employés pour les sensibiliser à la fraude doivent être mises en place afin de mieux cerner les contours de l'activité frauduleuse, sa prévention, sa détection et l'information à donner à ce sujet. C'est ainsi que les auditeurs internes et les entreprises pourront s'assurer l'aide des clients, employés, actionnaires et parties prenantes dans la lutte contre la fraude à tous les niveaux.

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. EVALUATION DE LA FRAUDE EN TANT QUE RISQUE DE L'ENTREPRISE

3.1 Les auditeurs internes abordent leur travail sous l'angle de l'évaluation du risque, et s'intéressent essentiellement aux risques majeurs pour l'entreprise, aux risques liés aux systèmes opérationnels et aux risques de défaut de contrôle. L'utilisation d'indices de risque est courante, notamment en matière de gestion de trésorerie. Des indices similaires peuvent être mis au point et utilisés pour prévoir les zones à risque en matière de fraude. L'activité inhabituelle d'un fournisseur, une soumission d'offre par un cartel et le train de vie des employés sont quelques exemples qui pourraient servir à élaborer un indice pondéré d'identification des besoins d'investigation, avant qu'une fraude ne devienne si importante ou répandue qu'elle n'entraîne un lourd préjudice pour l'entreprise.

L'effondrement en série de sociétés médiatiques est dû, pour la plupart, à un cas de fraude. La réduction des niveaux hiérarchiques et la recomposition des processus d'entreprise ont contribué à accroître l'exposition de ces entreprises aux risques et ont placé le risque très haut dans les préoccupations du conseil d'administration, du management, des auditeurs internes et des auditeurs externes. Le risque ne doit toutefois pas être considéré uniquement comme un danger. Le risque représente aussi une opportunité, et la prise de risques, à condition qu'ils soient calculés, fait partie de la culture des affaires, du marché et de l'entreprise. Tout entrepreneur le sait : *il n'y a pas de profit sans risque.*

Le risque est défini dans les *normes professionnelles* de l'IIA comme suit :

« La probabilité qu'un événement ou qu'une action ait des retombées négatives sur l'entreprise » (Norme 410.01.1b)

Toutefois, la véritable nature du risque peut être qualifiée de deux manières : objective ou subjective.

Le risque objectif comporte quatre éléments clefs :

- un danger ou une menace potentiel(le),
- la probabilité de réalisation de situations ou d'événements non souhaités,
- les conséquences ou l'impact d'une telle réalisation,
- l'exposition au risque – soit l'impact multiplié par la probabilité de réalisation.

Les risques sont de ce fait facilement quantifiables, dès lors que des valeurs monétaires peuvent être affectées à la probabilité de réalisation de situations ou d'événements non souhaités.

Un large éventail de facteurs psychologiques, culturels et sociaux façonne la perception du risque d'un individu à l'autre. C'est ce que l'on désigne par risque subjectif. Ces facteurs comprennent :

- Le contrôle : décidé de manière autonome ou imposé de l'extérieur,
- La crainte ou l'importance de l'impact,
- La familiarité,
- L'échéance : un risque à long terme est minimisé,
- Les facteurs de société tels que les groupes de pression,
- La confiance.

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.

3.2 Toutes les évaluations du risque sont, en pratique, un compromis entre science, valeurs et jugement et, si la plupart des observateurs estiment que certains risques ou dangers ne devraient jamais être courus, le reste du temps, il convient de minimiser les risques en prenant des mesures pour les contrer. La gestion du risque peut être comparée à la gestion et au contrôle financiers. Elle peut être utilisée de manière pro-active pour réduire les risques en essayant d'anticiper ce qui pourrait mal se passer et en cherchant activement à réduire la probabilité ou l'impact du risque.

La gestion du risque doit être pratiquée dans toute l'entreprise. On rencontre différents types de risques, à des degrés et niveaux variables, et à différents échelons de l'entreprise. La direction est concernée en priorité par les questions stratégiques relatives à l'orientation de l'activité et à la mise en œuvre de cette stratégie. Au niveau commercial, il s'agit de transformer la stratégie en plans d'action tactiques. La gestion de projet met en œuvre les plans tactiques au travers d'activités de développement, tandis que la gestion opérationnelle vise à réaliser ces plans en faisant fonctionner les services et les systèmes nécessaires pour fournir les produits ou prestations.

3.3 À chaque échelon, l'impact des risques de l'entreprise varie en fonction de l'objectif des fonctions et processus concernés. Cet impact peut être mesuré suivant l'un ou plusieurs des éléments suivants :

- Coût.
- Respect des délais.
- Qualité.
- Sécurité (dont hygiène).
- Confidentialité (notamment sur un plan commercial).
- Impact sur l'environnement.
- Image.

La possibilité de réalisation de la fraude à un niveau particulier, ou à tous les niveaux de l'entreprise, est un risque qui doit être reconnu par les responsables concernés, et qui doit faire partie de la gestion du « risk cycle ». Cette dernière revêt deux aspects essentiels :

- Identifier correctement les risques majeurs
- Vérifier que des stratégies sont mises en place pour les gérer.

L'analyse des risques et leur gestion sont intrinsèquement liées. L'analyse comprend les éléments suivants :

- Définition du contexte et mise en perspective.
- Identification et documentation des risques.
- Evaluation, quantification et classification des risques.
- Evaluation et modélisation du risque.
- Mise au point de stratégies de réduction du risque et de contrôle.
- Obtention de ressources et attribution des responsabilités.
- Réduction, transfert ou élimination du risque.
- Pilotage et suivi du risque.

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.

La position de l'ECIIA est la suivante :

- **La fraude, en tant que risque pour une entreprise, doit faire l'objet d'une attention particulière au plus haut niveau de l'entreprise, c'est-à-dire au cours de la revue stratégique par le conseil d'administration.**
- **Le danger de fraude au niveau stratégique ne devrait pas être perçu systématiquement comme un risque pour la continuité d'exploitation de l'entreprise, même s'il existe des exemples connus de sociétés qui ont dû cesser leur activité à la suite d'une fraude. Au niveau opérationnel, il existe des domaines pour lesquels l'impact de la fraude peut être important, soit isolément, soit collectivement.** ***L'évaluation et l'identification du risque doivent par conséquent impliquer les responsables à tous les niveaux de l'entreprise.***

L'ECIIA recommande fortement que le management reçoive une formation de sensibilisation à la fraude et, si nécessaire, à l'identification et à l'évaluation du risque de fraude.

3.4 L'audit interne a un rôle important à jouer à ce niveau :

- Le rôle de l'auditeur interne, dans son acception courante, est de fournir une « évaluation indépendante » de la pertinence, de l'application et de l'efficacité des dispositifs de contrôle interne mis en place par le management. **En ce qui concerne spécifiquement la fraude en tant que risque de l'entreprise, l'audit interne accomplit sa mission en examinant les dispositifs mis en œuvre par la Direction Générale et le management.**
- La valeur ajoutée de l'audit interne est de contribuer à l'amélioration des opérations de l'entreprise en facilitant l'identification et l'évaluation des risques à tous les niveaux. L'audit interne devrait y parvenir en examinant l'efficacité des processus de gestion des risques mis en place dans l'entreprise et en s'assurant de l'existence de procédures et de normes claires et cohérentes en matière de risque. **L'audit interne devrait garantir l'existence de forums de discussion adaptés sur les risques à tous les niveaux, une répartition clairement définie des responsabilités pour l'identification et l'évaluation des risques, ainsi que la mise en place de procédures appropriées pour la gestion et le suivi par le management.**
- L'audit interne apporte une garantie régulière et objective – surtout lorsque le risque peut être jugé critique. *L'audit interne doit être considéré comme une composante essentielle du système général de gestion des risques.*

La fraude est un risque de l'entreprise. Elle doit être évaluée avec tous les autres risques susceptibles d'avoir un impact sur la continuité d'exploitation de l'entreprise. En veillant à ce que l'audit interne, dans le cadre de son programme de travail normal, examine et rende compte du processus d'évaluation du risque à tous les niveaux de l'entreprise, la Direction Générale peut à la fois exploiter pleinement le potentiel de l'audit interne *et* apprécier utilement l'efficacité de ses propres processus.

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.

4. LE RÔLE DU CONSEIL D'ADMINISTRATION, DE LA DIRECTION ET DU COMITÉ D'AUDIT

4.1 L'évolution des principes de gouvernement d'entreprise en Europe et dans le monde entier met l'accent sur l'étroite relation entre le contrôle interne, l'équipe dirigeante en place et le concept de continuité d'exploitation. Autrement dit, les défaillances en matière de contrôle interne ont pratiquement toujours été identifiées comme l'un des principaux facteurs dans les nombreux effondrements d'entreprises qui ont marqué la fin du vingtième siècle. La culture de contrôle, pilier essentiel du cadre de maîtrise COSO *(The Committee of Sponsoring Organisations of the Treadway Commission : Internal Control – Integrated Framework USA 1992)*, émane des niveaux les plus élevés de l'entreprise. Souvent considérée comme une culture initiée par le haut de la hiérarchie, ses principes se répercutent à tous les niveaux hiérarchiques et s'incarnent dans la manière dont les employés exercent leurs activités individuelles. Ainsi, une activité inappropriée, douteuse ou même criminelle au niveau du conseil d'administration aura des répercussions dans toute la structure.

L'approche dite de « soft control » (contrôles informels), qui met l'accent sur les codes d'éthique, la culture et le comportement des pairs, dépend également de l'exemplarité donnée par la hiérarchie. Toutefois, dans ce cas, on se fie davantage à la responsabilité individuelle à tous les niveaux de l'entreprise pour avoir un comportement déontologique et socialement acceptable, qu'aux seules performances en salle de conseil d'administration *(CoCo – Criteria of Control Board – Institut Canadien des Experts-comptables agréés, 1995)*.

Une récente enquête publiée par l'AICPA (avril 1999, *COSO fraud review* 1987-1997) a montré que la falsification des comptes constituait l'activité frauduleuse la plus répandue au monde. Etant donné qu'elle ne peut intervenir qu'avec la complicité active de cadres de très haut niveau, quelle que soit l'entreprise, il est clair que l'honnêteté, la responsabilité et l'intégrité – toutes trois gages d'une bonne gestion – restent très menacées. L'activité frauduleuse, lorsqu'elle s'exerce à ce niveau, est difficile à déceler ou même à prévenir face à des administrateurs ou à des actionnaires puissants et déterminés.

Une enquête mondiale réalisée en 1998 par le cabinet Ernst and Young, intitulée *Fraud : the Unmanaged Risk*, a établi que 84 % des fraudes graves étaient perpétrées par les propres employés de l'entreprise. Si une grande partie de ces actions frauduleuses ont probablement été commises dans le but de tromper, il se peut également que certaines aient été le fait d'individus s'étant aperçu que des erreurs n'étaient pas détectées par le système et pouvaient être exploitées.

4.2 Trois grandes questions doivent être traitées à ce niveau :

- Dans quelle mesure les systèmes de contrôle interne peuvent-ils prévenir, dissuader et / ou détecter ultérieurement l'employé fraudeur.
- Dans quelle mesure des exigences accrues en terme de gestion et de contrôle – tant internes qu'externes – peuvent-elles empêcher la fraude à haut niveau.
- Dans quelle mesure l'audit interne peut-il rendre compte au comité d'audit, en vertu de sa Charte, des mauvaises pratiques de management.

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.

L'évolution des normes de reporting des sociétés constitue une particularité que l'on retrouve dans tous les rapports de gouvernement d'entreprise rédigés en Europe ces dernières années. Le Rapport Turnbull de 1999, au Royaume-Uni *(Contrôle Interne – Directives à l'intention des sociétés cotées en bourse et constituées au Royaume-Uni)* propose un rapport annuel sur le contrôle interne et pas seulement sur le contrôle financier. Cet accent mis sur le contrôle interne est en phase avec les précédents rapports britanniques : de Cadbury (1992), Hampel (1998) - bien que Hampel ait eu une position ambivalente sur tout ce qui sort du strict contrôle financier – et avec le '*UK Combined Code*' de 1999.

Il convient également de remarquer que le Panel Consultatif sur la Fraude *(Fraud Advisory Panel)* de l'Institut britannique des Experts-Comptables d'Angleterre et du Pays de Galles (ICAEW, *Institute of Chartered Accountants of England and Wales*) débat de la nécessité d'étendre les formes de communication recommandées par Turnbull. En d'autres termes, le rapport annuel et les comptes pourraient mettre l'accent sur une déclaration analogue à la déclaration portant sur les contrôles internes. Cela exigerait des administrateurs qu'ils divulguent, par exemple, le détail des systèmes en place pour combattre et détecter la fraude.

Des obligations similaires concernant les commentaires sur le contrôle interne existent déjà au Luxembourg pour les institutions financières et de crédit concernées (Circulaire 98/143 de l'IML), aux Pays-Bas, par suite du rapport du Comité sur le Gouvernement d'Entreprise, et en France où, après le Rapport Viénot, la réglementation a été renforcée pour les institutions de crédit. Ces dernières sont désormais tenues de présenter un rapport annuel « sur les conditions dans lesquelles le contrôle interne est réalisé ». La difficulté que présentent ces obligations de rapport, aussi louables soient-elles, est qu'elles risquent de n'être qu'un nouvel élément de « façade » qui reste soumis à la manipulation d'individus occupant un niveau hiérarchique élevé. Ce point a été martelé au Royaume-Uni par le Comité Consultatif sur la Fraude de l'ICAEW, dans son premier rapport annuel (1999), qui indiquait une fois encore que l'essentiel de la fraude est perpétré par des cadres haut placés.

4.3 Une façon pour le conseil d'administration de répondre au problème de la corruption et d'autres malversations, est la publication d'une prise de position relative à l'éthique dans les affaires et à la prévention de la fraude. L'objectif de cette procédure devrait être de délimiter les contours d'un comportement acceptable, définir les attentes et mettre en place des références pour aider les employés à évaluer leurs actions. Elle devrait être approuvée au plus haut de la hiérarchie, et diffusée à tout l'encadrement et au personnel. L'Annexe B présente les éléments à prendre en considération.

Le message fondamental qu'il convient de faire passer est le suivant : les employés travaillent dans un environnement régi par un ensemble de règles que tout le monde dans l'entreprise doit accepter, de la direction jusqu'aux employés. Les personnes qui dérogent à ces règles, et notamment celles qui commettent des fraudes, ne se rendent pas seulement coupables d'actes potentiellement criminels, mais travaillent activement à l'encontre des objectifs de l'entreprise et au détriment des intérêts de l'actionnaire.

Le corollaire essentiel du code de conduite, *selon L'ECIIA,* est un processus d'audit interne rigoureux à même de procurer un sentiment de sécurité aux parties prenantes en vertu de sa diligence. Si l'on exige seulement du commissaire aux comptes qu'il vérifie le processus par lequel le Président du conseil d'administration fait son compte rendu sur le contrôle interne et rend compte au conseil d'administration, on encourt le risque qu'un tel proces-

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), E*CIIA 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.

sus ne soit pas perçu par le public comme suffisamment transparent ou suffisamment rigoureux. Toutefois, même ce processus pourrait être amélioré si le commissaire aux comptes devait faire explicitement référence au travail de l'audit interne dans ce domaine.

4.4 La norme d'audit internationale 240 *(ISA, International Standard for Auditing)* définit des normes et donne des directives sur la responsabilité du commissaire aux comptes dans l'appréhension d'une fraude et d'erreurs lors de la certification des comptes. **L'ECIIA estime que l'examen actuel de l'ISA auquel se livre le Comité international des pratiques en matière d'audit *(International Auditing Practices Committee)* gagnerait à inclure une obligation explicite pour le commissaire aux comptes de prendre en considération le travail de l'auditeur interne, et de discuter toute conclusion importante avec lui. Il existe d'autres domaines dans lesquels l'ECIIA estime que sa contribution à une nouvelle norme ISA pourrait changer de manière significative sa valeur pour les commissaires aux comptes comme pour les dirigeants d'entreprise. L'Annexe C présente des commentaires spécifiques sur ce point.**

4.5 Dans sa réponse d'octobre 1996 au livre vert de la Commission Européenne intitulé *Rôle, statut et engagement du commissaire aux comptes dans l'Union européenne* (juillet 1996)[i], l'ECIIA déclare, entre autres, ce qui suit :

« L'établissement, la gestion et le maintien d'un système de contrôle interne efficace exigent des compétences que ne possèdent pas la plupart des dirigeants. »

Cette déclaration s'inscrit dans le cadre d'un débat qui concernait, à l'époque, une différence de perception sur les prestations délivrées par les commissaires aux comptes entre le public et les commissaires aux comptes eux-mêmes. Ainsi, un rapport « sans réserve » émis par un commissaire aux comptes était considéré par les parties prenantes comme une approbation, tant en matière de conformité juridique, d'absence de fraude et de continuité d'exploitation qu'en matière d'obligations écologiques et sociales. En d'autres termes, on considérait que le contrôle interne, tel qu'il avait été mis en place par la direction pour réaliser ses objectifs, était, est et serait toujours opérant.

Malgré les nombreux changements intervenus en terme de réglementation et de mise en conformité dans le domaine du gouvernement d'entreprise – lequel inclut la lutte contre la fraude – le contrôle interne est resté au cœur du débat. Le contrôle interne fait partie intégrante du processus de management. Il provient de la manière dont la direction et le management gèrent leur entreprise. Le rapport COSO définit le contrôle interne comme « … un processus appliqué par le conseil d'administration, le management et les employés, destiné à apporter une garantie raisonnable de la réalisation des objectifs » dans les domaines suivants :

- Efficacité et efficience des opérations,
- Fiabilité des états financiers,
- Conformité avec les lois et réglementations applicables.

Du point de vue du COSO, toutes les entreprises sont exposées à un risque, interne comme externe. Cette exposition est susceptible de nuire à leur pérennité, leur compétitivité, leur solidité financière et la qualité des produits, des services et du personnel. Il est clair que la fraude constitue un risque majeur à cet égard, qui peut affecter la continuité de l'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.

4.6 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.

Le programme de travail annuel de l'audit interne est orienté vers les risques auxquels l'entreprise est exposée et les risques identifiés dans chaque processus ou système soumis à l'audit. L'audit interne devrait aboutir à :

- Une opinion sur l'efficacité du contrôle interne présentée par le responsable de l'audit interne au comité d'audit.
- Une meilleure évaluation de l'état du contrôle interne par le comité d'audit, grâce à une interaction continue, tout au long de l'année, entre l'audit interne et le comité d'audit.

La position de l'ECIIA est la suivante :

Sans l'implication active du processus d'audit interne, on voit mal comment le conseil d'administration peut réunir suffisamment d'informations objectives pour s'acquitter de sa fonction de gestion, être conscient des risques de fraude ou rendre compte efficacement du contrôle interne.

4.6 L'ECIIA est convaincue que la direction reste tenue de mettre en place une structure de contrôle appropriée destinée à assurer la réalisation des objectifs de l'entreprise. La structure de contrôle devrait, entre autres, assurer la réduction des risques encourus par l'entreprise, y compris le risque de fraude. De plus, son efficacité devrait être réévaluée de temps à autre. L'ECIIA estime également qu'un bon comité d'audit a un rôle essentiel à jouer dans ce domaine mais, qu'en l'absence de formation et de sensibilisation, il sera incapable de réaliser un examen des processus et des risques encourus.

Le rôle de l'audit interne est de conseiller et d'aider la direction à s'assurer de l'efficacité du contrôle en mettant au point un programme de travail reposant sur les risques et couvrant les principales activités et les principaux systèmes de l'entreprise. L'audit interne devrait également veiller à ce que la Direction Générale et le management se sont donnés les moyens en terme de formation pour comprendre la complexité de la gestion du risque, du contrôle interne et de l'activité frauduleuse.

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.

5. LE RÔLE DE L'AUDITEUR INTERNE

5.1 Quelle contribution l'audit interne peut-il apporter à la prévention et la détection de la fraude ? Il est du ressort de la direction de mettre en place des systèmes et des processus à même de prévenir et de détecter les fraudes au sein de l'entreprise. L'audit interne peut les aider dans cette tâche, en :

- évaluant les risques et les stratégies de contrôle de l'entreprise,
- s'impliquant dans l'amélioration des stratégies de contrôle et la réduction du niveau des risques,
- s'assurant que l'organisation « contrôle » ses risques.

Par conséquent, l'audit interne doit en premier lieu examiner les éléments suivants au sein de l'entreprise :

- Attitude du conseil d'administration vis-à-vis du risque – par exemple, les dirigeants sont-ils disposés à prendre des risques, sont-ils au contraire réticents ou ont-ils opté pour une position intermédiaire, et comment cette attitude se répercute-t-elle dans l'entreprise ?
- Approche du risque – les risques majeurs dans les différents départements de l'entreprise sont-ils traités différemment (transfert, refus, assurance ou acceptation du risque par exemple) ?
- Systèmes globaux de gestion du risque – ceux-ci sont-ils intégrés dans les fonctions de l'entreprise, de manière à refléter et à représenter l'approche afférente au risque établie dans des domaines spécifiques ?

5.2 Les *Normes* professionnelles de l'*Institute of Internal Auditors* (IIA) exigent de ses membres qu'ils examinent les risques associés à la sauvegarde des actifs *(Norme 330)*. Il s'agit pour eux, dans le cadre de leur fonction, d'envisager en particulier les différents types de pertes engendrés notamment par le vol ou des activités inadéquates ou illégales. Ils devraient participer à la lutte contre la fraude en vérifiant la pertinence et l'efficacité du contrôle au regard de l'exposition au risque dans les différents segments d'activités de l'entreprise. Dans le cadre de cette mission, les auditeurs internes doivent déterminer si :

- L'environnement de l'entreprise favorise la sensibilisation au risque et au contrôle,
- Des objectifs d'entreprise réalistes ont été fixés,
- Des procédures écrites (codes de conduite) existent, qui décrivent les activités prohibées et les mesures à prendre en cas d'infraction avérée,
- Des procédures d'autorisation appropriées pour les transactions sont mises en place et maintenues,
- Des politiques, pratiques, procédures, rapports et autres mécanismes sont mis au point pour piloter les activités et protéger les actifs, en particulier dans les domaines à haut risque,

- 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.

- Des canaux de communication donnent à la direction des informations pertinentes et fiables,
- Des recommandations sont nécessaires pour établir ou améliorer des contrôles, à moindre coût, qui contribueront à dissuader les opérations frauduleuses.

Les entreprises évoluent dans un environnement dans lequel l'adaptation et l'amélioration continues sont la norme. Il importe donc que la direction mette en place des processus destinés à piloter, adapter et améliorer en permanence ses stratégies, structures et systèmes en matière de risque et de contrôle. En outre, la direction doit disposer d'une forme d'assurance lui garantissant qu'elle « maîtrise » les risques et les éventuelles fraudes auxquelles elle peut être exposée.

La position de l'ECIIA est la suivante :

L'audit interne est une composante essentielle du processus d'évaluation, d'amélioration et d'assurance à l'égard du risque, via :

- **La mise en place de plans d'audit reposant sur le risque.**
- **Son implication dans des projets stratégiques de conseil ;**
- **Sa contribution à la mise au point de nouveaux systèmes.**
- **L'introduction et la mise en œuvre d'un dispositif d'auto-évaluation des contrôles et des risques.**

5.3 L'audit interne aide la direction à réaliser ses objectifs, mais il peut également aider le comité d'audit à s'acquitter de ses responsabilités, en particulier dans les domaines du risque et du contrôle interne, de la fraude et des enquêtes internes. Les comités d'audit doivent regarder si le rôle de la fonction d'audit interne est approprié et s'assurer que cette fonction dispose de canaux de remontée d'information adéquats ainsi que de ressources correspondant à ses besoins. Une fonction d'audit interne forte, qui rend compte à un comité d'audit intéressé par l'amélioration de tous les aspects de la performance de l'entreprise, a un rôle important à jouer dans le maintien de systèmes de contrôle efficaces.

« Les sociétés qui ne disposent pas d'une fonction d'audit interne forte seront incapables de fournir à un comité d'audit suffisamment d'informations pour qu'il puisse s'acquitter de ses responsabilités. »

(Livre vert de la Commission Européenne sur l'Audit, 1996)

5.4 Pour que l'audit interne fournisse un service efficace, il est nécessaire que le conseil d'administration et le management comprennent la responsabilité qui leur incombe, à savoir :

- Définir le climat moral dans lequel évolue l'entreprise,
- Fournir la structure nécessaire pour permettre de réaliser leurs plans et de suivre leurs politiques,
- Appréhender son comportement face au risque et développer une stratégie de gestion du risque,
- Etablir et maintenir des contrôles internes,

- 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.

- Déterminer les ratios coût / contrôle en gardant à l'esprit l'équation : « exposition moins protection égale risque »,
- Etablir et maintenir les voies de communication et les systèmes de reporting au sein de l'entreprise pour savoir ce qui se passe.

Il incombe aux auditeurs internes de déterminer si toutes ces mesures ont été concrétisées et si elles sont exécutées avec efficacité et au moindre coût.

Les travaux entrepris par l'audit interne portent sur les risques auxquels l'entreprise est exposée et les risques identifiés dans chaque processus ou système à auditer. Le résultat de l'activité d'audit interne annuelle devrait être le suivant :

(a) une meilleure compréhension, au sein de l'entreprise, de la manière d'identifier et de gérer les risques susceptibles de donner lieu à une fraude ou à un abus,

(b) une opinion sur l'efficacité des contrôles internes, présentée par le responsable de l'audit interne au comité d'audit et au conseil d'administration,

(c) une meilleure évaluation de l'état du contrôle interne par le comité d'audit, grâce à l'interaction continue, tout au long de l'année, entre ce comité et l'audit interne.

La position de l'ECIIA est la suivante :

Toutes les sociétés européennes cotées en bourse – ainsi que les autres organisations concernées – devraient s'adjoindre les services d'une fonction d'audit interne disposant de ressources appropriées et d'un responsable de l'audit interne professionnellement qualifié qui rende compte aux plus hauts niveaux de l'entreprise, c'est-à-dire au conseil d'administration et au comité d'audit. C'est le meilleur moyen d'apporter aux parties prenantes l'assurance que des dispositifs d'évaluation et de contrôle du risque sont en place, et qu'ils sont à la fois pertinents et efficaces.

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.

6. RENDRE COMPTE D'UNE ACTIVITÉ FRAUDULEUSE

6.1 Tous les travaux d'audit interne ou externe ne permettront pas de déceler une fraude. De la même façon, le travail d'autres professionnels tels que des Experts Agréés en matière de Fraude *(Certified Fraud Examiners)* ne pourra pas non plus garantir sa détection. Les auditeurs internes ont toutefois l'avantage d'avoir une vision interne de l'entreprise. La suspicion ou la détection d'activités frauduleuses surviennent normalement de l'une des manières suivantes :

- Les conclusions du travail d'audit, ou
- Une découverte fortuite, ou
- L'expression de préoccupations d'employés de la société.

Toutes les structures de vérification – et l'audit interne en particulier – lorsqu'elles examinent les systèmes, devraient s'assurer qu'il existe des contrôles adéquats. Dans le cas contraire, elles devraient proposer des améliorations pour favoriser la mise en conformité avec les procédures et pratiques acceptables. Les améliorations suggérées peuvent comprendre des mesures de prévention, de détection ou de dissuasion de la fraude. Les auditeurs internes sont tenus, par leurs *Normes*, de faire preuve de « diligence raisonnable », c'est-à-dire de faire preuve d'un niveau de compétence et d'un soin tels que l'on est en droit d'attendre d'un professionnel de statut comparable. La diligence raisonnable ne signifie pas que les auditeurs internes doivent détecter toutes les fraudes, mais qu'ils doivent faire preuve d'un soin et d'une prudence raisonnables ; les auditeurs internes doivent être à l'écoute des erreurs et des irrégularités susceptibles de constituer des indicateurs de fraude.

6.2 Les employés de l'entreprise peuvent faire part de leurs suspicions de fraude et d'abus. Cette démarche est couramment appelée « dénonciation ». La dénonciation a fait l'objet de législations aux Etats-Unis, Australie, Nouvelle Zélande, et Royaume-Uni sur les dix dernières années. Pour être efficace, le système de dénonciation doit comprendre :

- Une déclaration nette que toute action frauduleuse est prise au sérieux dans l'entreprise, et une indication des types d'actions considérées comme relevant de la malversation,
- Le respect de la confidentialité vis-à-vis de l'employé qui aurait fait part de sa préoccupation, s'il le souhaite,
- La possibilité de faire connaître ses préoccupations en outrepassant la ligne hiérarchique,
- Des pénalités en cas d'allégations fausses ou calomnieuses,
- Une indication de la manière dont les préoccupations peuvent être exprimées en dehors de l'entreprise, si nécessaire.

Une bonne pratique de gestion consiste à s'assurer que le personnel a été informé de façon formelle de voies d'expression suffisantes pour communiquer ses préoccupations en interne, au sein de l'entreprise, et qu'il existe des procédures solides permettant de traiter de manière exhaustive toutes les préoccupations exprimées.

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.

La position de l'ECIIA est la suivante :

L'audit interne peut être utilisé par le personnel comme une alternative au processus hiérarchique pour exprimer ses préoccupations en toute confidentialité. Il importe toutefois que le conseil d'administration indique clairement de quelle manière il souhaite que l'audit interne traite ces questions. A son tour, l'audit interne devrait strictement se conformer aux procédures approuvées.

Pour aider le personnel à exprimer ses préoccupations, de nombreuses entreprises ont adopté une procédure en matière de dénonciation. Les principaux éléments d'une telle procédure sont présentés en Annexe B.

6.3 Si, par suite du travail d'audit ou de préoccupations du personnel, l'audit interne soupçonne une fraude, il devra étudier l'opportunité d'en informer le responsable hiérarchique concerné. Cela peut être fait verbalement ou par le biais d'un rapport écrit, provisoire ou définitif, contenant les éléments découverts et concluant sur l'existence d'informations suffisantes ou non pour mener une investigation complète. Les conseillers juridiques de l'entreprise peuvent être consultés avant la préparation d'un rapport écrit.

En ce qui concerne les délais, les responsables hiérarchiques concernés devraient être informés dès que possible en cas de soupçon fondé de fraude. Ils devraient également être informés immédiatement si l'on juge que la fraude affecte de manière importante des comptes publiés antérieurement.

Il est important que l'auditeur interne identifie qui peut ou ne peut pas avoir été impliqué dans une fraude interne, de manière à s'assurer que la diffusion d'un rapport n'alerte pas les coupables. Si les personnes impliquées sont alertées, toute poursuite de l'affaire risque d'être compromise si ces personnes ont la possibilité de modifier ou de détruire les preuves. Une information prématurée peut également permettre aux coupables de réaliser le produit de leur fraude et de le dissimuler.

Le rapport écrit établi à la fin de cette phase devrait comprendre tous les éléments découverts, toutes les conclusions et les recommandations, ainsi que toutes les mesures correctives qui auront été prises. Il peut également être soumis à l'examen des conseillers juridiques de l'entreprise.

6.4 Un élément important à prendre en considération concerne les circonstances dans lesquelles, et le moment où, les soupçons ou les preuves de fraude devraient être portés à la connaissance des autorités réglementaires extérieures ou de la police. Lorsque l'entreprise dispose d'une fonction spécialisée dans le traitement de la fraude, elle doit également se doter d'une procédure et d'un protocole de déclaration impliquant les conseillers juridiques de l'entreprise.

Si tel n'est pas le cas, et si la fraude est découverte par suite du travail d'audit interne ou si elle a fait l'objet d'une investigation par l'audit interne à la demande de la direction, les conseillers juridiques de l'entreprise devraient être consultés dès l'apparition d'un soupçon raisonnable qu'une fraude a été commise.

L'absence d'investigation adéquate sur la fraude ou la non obtention d'une preuve légalement valable pourrait compromettre toute poursuite ultérieure. Si l'auditeur interne ou un autre enquêteur interne n'est pas parfaitement familiarisé ou suffisamment expérimenté avec les règles applicables aux preuves, il est impératif d'informer la police dès qu'il existe un soupçon fondé, afin que tout risque puisse être évité.

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.**

6.5 L'enquête sur la fraude est le rôle d'un spécialiste. L'auditeur interne peut mener une investigation sur la fraude, mais seulement s'il dispose de l'expertise et de l'autorité adéquates. Dans certaines entreprises, il existe des équipes spécialisées dans ce type d'enquêtes, soit au sein de la fonction d'audit interne, soit en dehors de celle-ci. Normalement, l'audit interne aide ces équipes spécialisées dans leurs investigations.

La position de l'ECIIA est la suivante :

Les auditeurs internes peuvent jouer un rôle important en matière d'enquête sur la fraude, car :

- **Ils ont un mode de réflexion objectif et ils sont habitués à s'appuyer sur des faits et des analyses objectives,**
- **Ils comprennent la nature du contrôle et peuvent évaluer son efficacité. La fraude et l'abus surviennent lorsque les contrôles sont faibles et inefficaces. L'auditeur interne doit connaître les systèmes en place au sein de l'entreprise, et être capable d'identifier précisément les faiblesses qui ont été exploitées,**
- **Ils sont en droit d'interroger les fichiers d'applications et les journaux des systèmes afin de prouver ce qui s'est produit,**
- **Ils comprennent la notion de preuve ou de « piste d'audit » et la manière dont celle-ci peut être sécurisée. Les auditeurs internes doivent savoir quelle piste d'audit existe, sous quelle forme elle est conservée, de quelle manière elle est établie et quelle période de rétention est 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.

ANNEXE A

ETHIQUE DES AFFAIRES ET FRAUDE (MODÈLE DE PROCÉDURE)

Présentation des éléments à traiter

- Déclaration présentée par le Président du conseil d'administration / Directeur Général soulignant l'engagement de l'entreprise en faveur des critères éthiques les plus rigoureux et exigeant de tous les employés qu'ils prennent connaissance des procédures et directives publiées en matière de conduite d'entreprise et qu'ils s'y conforment.
- Nécessité pour tous les employés de respecter toutes les lois et tous les règlements applicables sur le lieu de travail.
- Directives en matière de cumul avec d'autres fonctions, telles que des charges d'administrateur hors de l'entreprise, ainsi qu'en matière de réalisation d'opérations personnelles au sein de l'entreprise ou susceptibles d'affecter l'entreprise ; ces directives doivent traiter notamment des questions relatives aux conflits d'intérêt.
- Lorsque l'entreprise ouvre son capital au public, exigence imposée aux employés ayant connaissance d'informations susceptibles d'avoir un impact sur le cours de l'action de se conformer aux codes de pratique relatifs au délit d'initié.
- Nécessité de se conformer aux procédures relatives à la sécurité et à la confidentialité des informations.
- Procédures relatives au paiement de gratifications, de cadeaux et de frais de représentation, ainsi qu'à l'acceptation de ces cadeaux et réceptions.

Les sujets à aborder dans la procédure se rapportant expressément à la fraude doivent comprendre :

- Déclaration selon laquelle les employés doivent toujours agir avec intégrité à tout moment et s'abstenir de toute activité frauduleuse, même si elle peut bénéficier à la société.
- Affirmation claire selon laquelle la procédure concerne tous les membres du personnel, sans considération de grade ni d'ancienneté.
- Engagement destiné à s'assurer que des contrôles et des procédures économiques seront mis en place pour prévenir, détecter, dissuader et traiter la fraude.
- Déclaration indiquant qu'il incombe à chaque employé de protéger les actifs de la société.
- Déclaration selon laquelle tous les employés doivent œuvrer en faveur du respect d'un niveau d'hygiène et de sécurité adéquat dans leur environnement de travail.
- Exigence selon laquelle tous les employés doivent comprendre et utiliser les procédures évoquées dans la section susmentionnée quant aux « systèmes destinés à encourager et à canaliser l'expression des préoccupations en matière de fraude ».
- Déclaration indiquant que les relations avec les institutions gouvernementales ne doivent violer aucune directive en matière d'éthique et d'intégrité.

- 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.

- Déclaration indiquant que toute communication hors de l'entreprise doit être adéquate, appropriée et exacte, et ne doit être faite que par les voies autorisées par l'entreprise.
- Attribution des responsabilités en matière d'investigation de fraude ou de mauvaise conduite présumée et définition des procédures de remontée d'information en interne qui s'appliquent en cas de fraude.
- Obligation pour tous les employés d'apporter leur aide à toute investigation si leur contribution est sollicitée.
- Procédure à appliquer en matière de mise à pied, de licenciement et de déclaration à la police en vue de poursuites (étant entendu que si la procédure prévoit de signaler toutes les affaires à la police, elle ne pourra être modifiée qu'avec l'accord exprès du Directeur Général ou d'un autre membre de l'équipe de direction).
- Engagement à recouvrer les fonds concernés par une procédure contentieuse.
- Exigence de veiller à ce que tout le personnel soit informé de la politique afférente à la conduite des affaires et à la lutte contre la fraude dès sa prise de fonctions, et à ce que tous reçoivent une copie de l'énoncé de cette politique, qu'ils devront signer afin d'attester qu'ils en ont pris connaissance et qu'ils consentent à en respecter la teneur. Un exemplaire devra être inséré dans le livret d'accueil remis aux membres du personnel.

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.

ANNEXE B

DENONCIATION (MODÈLE DE PROCÉDURE)

Présentation des éléments à traiter

- Portée de la déclaration destinée à couvrir les cas de fraude, de corruption et de faute professionnelle, de comportement criminel ou illégal, de déni de justice, de dommages concernant l'hygiène et la sécurité, etc.

- L'entreprise s'engage en général à adopter les normes les plus sévères et, en particulier, à impliquer le personnel dans la mise au point de ses procédures relatives à la remontée confidentielle d'informations. Elle s'engage à assurer le suivi de la procédure, à tenir des dossiers confidentiels sur toutes les affaires portées à son attention par le biais de la procédure de dénonciation, et à s'assurer qu'un comité approprié reçoit des rapports comportant une évaluation de l'efficacité de la procédure et de tout mode opératoire émergent.

- Encourager les employés à faire part de leurs préoccupations, en mentionnant la possibilité de se présenter avec un collègue ou une autre personne. Il doit y avoir une promesse de soutien et de confidentialité dans la mesure du possible, et cette démarche ne doit pas être décrite comme une infraction à la discipline pour ne pas dissuader le personnel de faire connaître ses préoccupations ; en outre, l'auteur d'une telle démarche ne doit pas subir de représailles pour avoir exprimé ses préoccupations. L'entreprise doit expressément s'engager à garantir que le fait pour un individu d'exprimer ses préoccupations n'entravera pas sa carrière.

- Les employés sont encouragés à « tirer la sonnette d'alarme » au sein de l'entreprise plutôt que d'ignorer un problème ou de l'évoquer à l'extérieur. Il est rappelé aux employés que les règles de l'entreprise leur imposent de ne pas divulguer d'informations confidentielles, fausses ou trompeuses. Le texte doit insister sur le fait que la divulgation faite dans l'intérêt public s'accompagne d'une protection légale pour les dénonciateurs qui sont honnêtement et raisonnablement convaincus de l'exactitude de leurs allégations et des informations qu'ils divulguent.

- Les employés soucieux d'exprimer leurs préoccupations doivent pouvoir disposer d'instruments de communication souples. Dans la plupart des cas, ces préoccupations devront être rapportées au supérieur hiérarchique direct. Il sera toutefois également possible dans certaines circonstances de s'adresser directement au service d'audit interne, à un dirigeant ou au directeur des services centraux, voire au directeur général. Cette option est laissée à la discrétion de la personne concernée. Le personnel a le droit de solliciter un entretien confidentiel, et il lui est rappelé que les deux parties doivent en respecter la confidentialité.

- Il existe parfois des circonstances exceptionnelles dans lesquelles il peut être préférable de contacter une entité externe.

- Il convient de veiller à ce que toutes les préoccupations soient étudiées attentivement et exhaustivement et traitées de manière appropriée. Des dispositions doivent être prises pour la réalisation d'investigations internes ou indépendantes. Toutes les parties doi-

- 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.

vent recevoir l'assurance de se voir traiter avec équité. Le cas échéant, l'entreprise doit accepter d'essayer de tenir la personne concernée informée des résultats des investigations et des mesures envisagées.

- L'entreprise s'engage à donner suite à toute préoccupation qui lui aura été communiquée dans les plus brefs délais, en indiquant la manière dont elle envisage de traiter l'affaire et selon quel délai. Si la décision de ne pas enquêter est prise, celle-ci doit être justifiée. La personne concernée est assurée de recevoir autant d'informations que possible sur les résultats de l'investigation, sous réserve de certaines limites.

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.

ANNEXE C
ISA 240 - COMMENTAIRES

Article 5. Responsabilité du management

Cet article peut être amélioré par l'ajout de commentaires relatifs (1) à l'utilisation d'une fonction d'audit interne efficace et professionnellement qualifiée et (2) à la mise en place par le conseil d'administration d'un code de déontologie.

Article 7. Evaluation du risque

Une bonne relation entre les auditeurs internes et externes contribuera à réduire le risque de fraude et d'erreur. Cet article peut être modifié pour s'assurer que le commissaire aux comptes statutaire discute activement avec l'audit interne des opinions de ce dernier sur le processus de gestion du risque et l'efficacité des systèmes de contrôle interne.

Article 14

Cet article doit prendre en compte l'existence d'un code déontologique et d'une procédure d'alerte interne qui permettraient de faire part de préoccupations en toute confidentialité à l'audit interne ou à une autre entité de vérification, et ainsi d'éviter la possibilité de contourner la hiérarchie.

Articles 17 et 18

Il est essentiel que le commissaire aux comptes informe le comité d'audit de l'existence possible d'une fraude ou d'une erreur révélée par le travail d'audit.

Articles 21, 22 et 23

Les circonstances entourant toute limitation de l'indication de fraude ou d'erreur aux utilisateurs du rapport de l'auditeur doivent être mentionnées de manière explicite.

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

Remerciements

L'ECIIA remercie les coordinateurs de cette prise de position pour leur travail :

Marian Lower, Royaume-Uni

Neil Cowan, Directeur Général, ECIIA

ainsi que les membres du Groupe de Projet de l'ECIIA pour leur participation :

Louis Vaurs, France

Dr. Peter Diekman, Pays-Bas,

Carolyn Dittmeier, Italie,

Einar Dossland, Norvège.

L'ECIIA souhaite également remercier l'*Institute of Internal Auditors – UK & Ireland*, institut britannique et irlandais de l'audit interne, pour la large utilisation des Notes 12 et 13 de l'exposé « Professional Briefing » intitulées : *Fraud and the Internal Auditor* (La fraude et l'auditeur interne) et *Managing Risk* (Gérer le risque), le UK charity Public Concern at Work (association britannique pour l'expression sur le lieu de travail) pour le modèle de procédure de dénonciation, et l'*Institute of Internal Auditors*, *Inc.*, pour les extraits du document *The Competency Framework for Internal Auditing* (le cadre de compétence de l'audit interne).

L'ECIIA a déjà publié une prise de position intitulée *Internal Auditing in Europe* (L'audit interne en Europe, 1996). Les instituts d'audit interne des pays de la région économique et géographique constituée par l'Europe et par le bassin méditerranéen peuvent adhérer à l'ECIIA. L'organisation compte actuellement 28 organismes membres.

The European Confederation of
Institutes of Internal Auditing

Meir 24
2000 Antwerp
Belgique

Tél. : +323 232 17 82
Fax : +323 226 68 02

[i] Traduction officielle de la Commission

Imprimerie Compédit Beauregard S.A./61600 LA FERTÉ-MACÉ
N° d'Imprimeur : 6491

L'activité **Recherche de l'Institut de l'Audit Interne,** ouverte à tous les adhérents, est l'expression du caractère associatif de l'Institut et concrétise notre devise : « Le Progrès par le Partage ».

La Recherche s'organise autour de **groupes de travail** qui mettent en commun et formalisent leurs réflexions et leurs pratiques sur un thème ou un sujet propre à un secteur d'activité.

Les travaux de ces groupes sont destinés à être diffusés sous de multiples formes auprès du plus grand nombre.

Telle est précisément la vocation de la Collection :

« Les Cahiers de la Recherche »

qui met à la disposition des auditeurs trois types d'outils :

- les « **Prises de Position** » publiées par des instances professionnelles,
- les « **Notes Professionnelles** » qui explicitent et commentent ces prises de position,
- les « **Guides d'Audit** » qui définissent un cadre pratique pour la conduite des missions.

IFACI Institut de l'Audit Interne

40, avenue Hoche, 75008 Paris. Tél.: 01 53 53 59 00, Fax : 01 45 62 40 89
Web : www.ifaci.com, E-mail : institut@ifaci.com
Institut Français de l'Audit et du Contrôle Internes. Association Loi 1901 - Siret 775 667 231 00069
The Institute of Internal Auditors