ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΟΙΚΗΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΜΟΝΑΔΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Management of internal fraud cases

Ροβέρτος Ρίβανς

Επιβλέπων καθηγητής: Παναγιώτης Αλεξάκης

ΑΘΗΝΑ
Ιούλιος 2018

Table of contents

1. Abstract

The purpose of this study is to show ways to manage internal fraud cases in terms of a business, as well as the contribution of the Internal Audit Unit of the company in this process.

An internal fraud issue is, usually, revealed after a long time but causes, in a very short time, a huge negative impact on the entity.

Therefore, it is critical for the enterprise to be prepared of how to handle potential internal fraud cases and to have the right and competent people to manage fraud issues in the best possible way.

The role of Internal Audit in such cases is crucial, since it doesn't only investigate the fraud, but at the same time provides significant assistance in the overall management of the internal fraud case.

2.Analysis of the theoretical foundations of the study

2.1 Fraud – definition and theories

Definitions

The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery (offering, requesting, or accepting bribes and other improper financial advantages) and extortion (blackmail).

Fraud is defined as the dishonest and intentional misappropriation of assets, services or benefits, or misrepresentation of financial condition (1).

Fraud also occurs when dishonest acts are committed without personal gain, but are intended to create a loss or risk of loss for another person or entity.

Fraud by means of misrepresentation occurs when a person intentionally does not disclose information in order to deceive the owner of benefits, assets, or services or to create a loss or risk of loss.

Fraud as defined in Article 386 of the Greek Penal Code: "Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by convincing a person to perform or omit or tolerate an action by representing false facts as true, or by unlawfully hiding or suppressing true facts, shall be punished with imprisonment for at least three months; and if the damage is exceptionally large with imprisonment for at least two years."
Similar provisions exist in all countries' Penal Codes.

Enablers of committing Fraud:

- Trust & Confidentiality play key role in the financial services business.

  When the client develops a comfort level with an employee (and vice versa) there is a greater opportunity for fraud to take place as verification and transactions checking are minimized.

For example, when you are learning how to drive, you drive safely and responsible all times. As you become more confident as a driver, your tendency is to be less careful and attentive which may result in an accident.

- Work in current position for a long time is considered as one of primary cause committing fraud by the insiders.

- Lack of Product Knowledge, Internal Processes and Minimal Experience may make an employee more vulnerable to fraud scheme.

  Inexperienced managers & employees may not have sufficient exposure to the operational processes, put more emphasis on productivity and may not fully understand the need for audit trails, control checks and verification processes.

  Lack of experienced and trained employees increases the factors that enable fraud to occur.

- Workplace Vulnerabilities: Inefficient rules, policies & regulations or/and weak internal & prevention controls. Lack of segregation of duties, work load and staff shortage are usually the circumstances that unethical and fraudulent behaviors are very likely to occur.

- Customer's/ Outsider's/ Insider's Economic Status (financial difficulties)

- Avoid Rules & Regulations

Also, there are some facts (3) which should be taken into consideration:

- Global economic downturn (there is a clear link between fraud patterns and changing economic circumstances)
- Legal framework is not able to cope with all of the white-collar crime
- Fraud -in general organized financial crime- has been become more sophisticated
- Controls & systems becoming outdated by new schemes
- Financial products and processes are more complex
- Traditional Ethical values have been challenged
- Fraud prevention culture is still maturing

The Fraud Triangle Theory

The Fraud Triangle, developed by American Criminologist Donald Cressey (7), is one of the models that demonstrates what are the circumstances or factors that unethical and fraudulent behaviors are very likely to occur:

- PRESSURES/NEED: The person is under very strong pressures: financial difficulties (needing money, family unemployment, overwhelming medical bills, high level of debts), work related (hiding mistakes, achieve targets, performance pressure, passed over for a promotion, feeling overworked and underpaid), personal (gambling, alcohol or drug addiction) or simple just greed (usually associated with injustice "I am not paid what I am really worth").

- OPPORTUNITIES: The person has the authority and the means to make the cheating possible: established trust (to ourselves, colleagues, manager, customer), weak or nonexistent controls, lack of segregation of duties.

Temporary situations where there is a chance to commit the act with a low chance of being caught.

Usually circumstances that processes are not followed due to workload, staff shortage or timeline pressures.

- ETHICAL RATIONALIZATION: is the ability to justify dishonesty and that is what makes the act possible; nobody likes to think about himself as a fraudster, he therefore must be able to rationalize his unethical or fraudulent behavior: “I am only borrowing the money, I will give it back when my financial situation improves”, “I need the money more than the “big” company”.

  The individual must first convince themselves that their behavior will be temporary or is acceptable.

The Fraud Diamond Model

The Fraud Diamond, a newer theory of fraud proposed by David T. Wolfe and Dana R. Hermanson, asserts that the fraudster's capability must also be taken into account.

The fraudster, it is said, must have the required traits (e.g., greed, weakness of character, excessive pride, dishonesty, etc.) and abilities (e.g., knowledge of processes and controls) to actually commit the fraud.

It can be argued, however, that traits are components of pressure and that abilities are opportunity factors.

The 10-80-10 Rule -National Association of State Auditors, Comptrollers and Treasurers (NASACT) and the Oregon State Controller’s Division- supports the general assumption of capability by breakdown of the population and the likelihood of fraud occurrences.

Essentially:

- 10 percent of the population will NEVER commit fraud. This is the type of person that will go out of their way to return items to the correct party.
- 80 percent of the population might commit fraud given the right combination of opportunity, pressure, and rationalization.
- 10 percent of the population are actively looking at systems and trying to find a way to commit fraud.

2.2 Fraud Risk Management - Policy and Principles

Fraud Risk Management Policy and Procedures should be in place, prescribing the Fraud Risk Management framework, aiming at protecting from both Internal and External Fraud incidents.

In parallel said policy and procedures should aim to ensure the existence of appropriate organizational structure and procedures for the Prevention, Detection, Investigation and Communication of Fraud Incidents [4, 6, 13].

Key policy elements should include the following:

- PREVENTION Involves the adoption of suitable mechanisms, the development of control procedures and practices at multiple levels within the company, as well as the fraud awareness of the employees on a regular basis.

- DETECTION Involves all controls which are adopted, in order to mitigate Operational Risk and also contribute to the detection of Operational Fraud (e.g. confirmations of transactions, internal & external reconciliations, exception reports, physical inspections and counts, data and documentation verifications, etc.)

- INVESTIGATION & CORRECTIVE ACTION Is initiated whenever events entailing well-founded suspicions of Fraud are captured by the Fraud Detection procedures. It follows specific rules and principles.

- COMMUNICATION AND INFORMATION DISSEMINATION Involves the notification of relevant issues within the Group as well as external stakeholders (Customers, Counterparties, Authorities, Mass Media if required)

Fraud (internal & external) create not only a financial loss & risk, but if not effectively addressed can also create legal (incl. fines, sanctions and financial penalties, increased litigation risk for the company and the involved employee/s that may also include employees dismissal; even though may unwittingly or carelessly get involved in a fraud) and reputational risk (bad media brings competitive disadvantage and inevitably losses) for the Company.

The company should take all required and reasonable measures to Prevent, Detect, Recover & Respond effectively to fraud against the Company and its Clients. More specifically:

- Prevent: Code of Ethics, Segregation of Duties, Information Security Framework, authorization & Verification Policies, Customers/Associates/Suppliers/ 3rd parties Due Diligence, KRIs, Fraud Risk Controls Processes, Fraud Risk Assessment, Fraud Awareness Training, Expense Claims & Hiring processes etc.

- Detect: Whistleblower Program, Regular and Special Audits, Fraud Examinations & Targeted Investigations

- Respond/ Recover: Legal Criminal Prosecution, Civil Action to Recover Funds, Employee's Disciplinary Actions, Enhance Internal Controls, Root Cause Analysis.

Establishing & Promoting a Control Environment

- Code of Ethics: Establishes the guiding principles of the company, sets the ethics and the key commitments towards Customers, Shareholders, the Community and its Personnel.

  It promotes honest and ethical conduct, compliance with applicable laws and regulations, and prompt reporting of violations of the code.

  It also confronts any possible Conflict of Interest such as accepting-giving gifts, any outside professional relationship or personal investments and in general any private interest that may interfere with the official responsibilities.

- Implementation of Whistleblower Program: Process and tools of communication any serious irregularities, omissions or offences that have come to the attention of the Personnel, including potential Fraud.

- Effective Personnel Related Policies: Hiring and Promotions policies (establishing standards for hiring and promoting the most qualified individuals; performance appraisals records); Evaluating Performance and Compensation Programs; Expense Claims policy; Defined roles and responsibilities.

- Targeted Antifraud Programs and Controls : Fraud investigations; Information Systems, Technology & Security controls, Tools to identify potential fraud schemes and scenarios; reviews on operating performance and security of assets; appropriate internal controls; complains process.

- Regular & Targeted Fraud Awareness Training: Provide anti-fraud training to all employees (incl. senior staff) especially those in high-risk areas; Internal Memos (highlighting new trends, red flags etc.).

2.3 Internal Fraud (types, impacts)

Internal fraud, also called *occupational fraud*, can be defined as: "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets" (1,10)

Simply stated, this type of fraud occurs when an employee, manager, or executive commits fraud against his or her employer.

The most common reasons for an employee to commit fraud are:

- Living beyond one's means
- Experiencing financial difficulties (debts, losses)
- Gambling/other addictions
- Greed

The three major types of occupational fraud are: Corruption, Asset Misappropriation, and Fraudulent Statements, which form the so called "Fraud Tree".

More specifically:

- Corruption schemes are those, in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit (e.g. schemes involving bribery or conflicts of interest).

- Asset misappropriation schemes are those, in which an employee steals or misuses the organization's resources (e.g., theft of company cash, false billing schemes or inflated expense reports)

- Financial statement fraud schemes are those, in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g., recording fictitious revenues, understating reported expenses or artificially inflating reported assets)

Most common types of internal fraud are the following:

- Theft, embezzlement and misappropriation of assets.
- Deliberate concealment or falsification of facts, transactions, financial reports (resulting in unreliable or distorted financial information) and data, including the context of concealment, with the intention to delay or avoid the detection of fraud.
- Unauthorized, illegal use or leakage to external parties of confidential or proprietary information for own benefit.
- Electronic Fraud, unauthorized use of systems and infrastructure.
- Unauthorized, preferential management of customers, suppliers, counterparties by breaching internal guidelines and policies (associated with bribery).
- Creation of fictitious customers or use of customer data to issue loans and cards.
- Falsification or forgery of payment instruments.

Impacts of internal Fraud

Internal fraud, despite the continuous strengthening of the safeguards and controls and the preventive measures taken from the part of businesses to avoid it, still arises and is usually revealed after a significant time delay, while in the meantime may cause a huge negative impact to the business.

It is quite clear that, after an internal fraud incident, the company has experienced the impact of three basic risks, financial, operational and reputation risk.

One of the main impacts for the business, usually measurable, is the economic loss, the size of which may significantly affect or jeopardize its viability.

Also, the disclosure of such an incident, if it becomes broadly known (publicity from the Mass Media and Press), causes defamation of the business and leads those individuals or entities, who have any kind of business transactions with the certain company, in loss of confidence.

The consequences of lost confidence are loss of market share, loss of revenues, economic contraction and, in some cases, collapse and permanent cessation of operations, with all the sequences that this implies for shareholders, suppliers, partners and, of course, the employees of the company (they would soon be unemployed).

It is understood that the above mentioned impacts and sequences are not measurable, but may result in greater damage than the financial losses.

2. Empirical analysis

3.1 Reasons for not timely revealing internal fraud

In the internal control system of a company, mechanisms are incorporated to prevent and detect internal fraud events, embedded in the work documented policies, procedures and regulations of Operating Units of the company.

The main mechanisms of fraud prevention are dual control, segregation of duties, predefined limits of liability, AML system (in credit institutions) etc.

The firm must have mechanisms and procedures for continuous monitoring "sensitive" transactions incurred by employees in the performance of their work, that possibly cover fraud activity and illegal benefits.

Based on the Association of Certified Fraud Examiners' Report to the Nations[(3)], the most common controls for preventing and detecting fraud are:

- Anti-fraud policy
- Code of conduct
- Dedicated fraud department function or team
- Employee support programs
- External audit of financial statements
- External audit of internal control over financial reporting
- Formal fraud risk assessments
- Fraud training for employees
- Fraud training for managers/executives
- Hotline
- Independent audit committee
- Internal audit department
- Job rotation/mandatory vacation
- Management review
- Management certification of financial statements
- Proactive data monitoring/analysis
- Rewards for whistleblowers
- Surprise audits.

It is crucial to develop relevant scenarios detecting possible fraud, in connection with the extraction and data analysis - data processing through appropriately structured information systems from specialized persons, who will be acting under the strictest confidentiality.

However, despite of all monitoring programs, procedures, regulations, safeguards and checkpoints at each stage of the work, it's a fact that internal fraud events still occur and, meanwhile, are revealed after significant time and not at the early stage, when the illegal activity of the fraudster could, naturally, be terminated and the incidence of fraud against the company could be reduced.

It is common secret that "the fraudster is always at least one step ahead of his/hers pursuers."

The reasons why fraud is not prevented or timely disclosed are many.

The fraudster employee is not necessarily a person with excellent skills and knowledge, or has an IQ well above average, he or she simply exploits some situations, both to commit and conceal fraud, so as not to be easily and immediately understood and revealed by those persons, with whom he/she shares his/hers work environment (colleagues, superiors or clients).

From a 25 years' experience in investigating cases of internal fraud at a financial institution, it came out as a conclusion that the most common internal fraud incidents are related to:

- Embezzlements in domestic or foreign currency from customers' deposit accounts, without the account holder's knowledge or consensus and by forging their signatures (most of the times this was connected with elderly abuse).

- Irregularities in issuing and approving credit cards and consumer or business loans in the name of customers but without their knowledge or approval, by using data and elements taken from their personal information files, which were kept electronically in the bank's information systems, by forgery of their signatures on application forms and related contractual documents and, after that, by using the relevant approved credit limits for the benefit of the employee or a third person, sometimes relatives or close friend of the fraudster.

- Irregular takeover of customers' investment products (e.g. mutual funds, time deposits, stocks) by the fraudster employee, with forged signatures on the relevant transaction documents.

These incidents were not detected at an early stage, mainly because:

- In the vast majority of cases, the existing guidelines and internal regulations for cash management, transactions control and reconciliations were not followed by the fraudster's superiors.

  This was because those persons (managers, supervisors), who were responsible for controlling the fraudster employee's transactions, either did not know well the relevant procedures, or did not implement due and thorough scrutiny of his/hers work, due to over confidence in him/her.

- The fraudster had gain the full confidence of the transacting customers and, taking advantage of this trust, was conducting irregular transactions in their accounts without their knowledge and consent and, basically, without their presence, removing various amounts from their accounts for his/hers own benefit.

  In the name of above mentioned trust and pretending that he/she is acting for the customer's good service and convenience, the fraudster persuaded and convinced the account holders to sign "blank" transaction documents (which then he/she used without the customers' knowledge, for misappropriation of their assets) or contractual documents, which were used on the issue of increased credit limits, the use of which was handling by the fraudster employee for his/hers benefit.

- Customers, in most cases elderly, or relatives of the fraudster, or residents abroad, had asked for service in the above manner, which made it easier for them, since they would not have the obligation to appear personally for all transactions, or authorize another person to act on their behalf, and had agreed to carry out their transactions in the above manner, without mentioning it to anyone else except the fraudster (e.g. to a senior officer of the credit institution), since they knew that this kind of service was not regularly provided and not permitted.

- The fraudster, exploiting the poor or not at all control of his work by his superiors, had improperly connected customers' deposits accounts to his own web banking profile and, through this connection, was conducting money transfers to his/hers deposit accounts through web, using PCs located outside his workplace (whether his/hers home personal computer, or personal computers with public use in specialized stores (e.g. internet café).

- In most cases the fraudster employee falsified the customer's signature in transaction or contractual documents, misleading his/hers superiors by convincing them that the signatures of the customer were put in front of him.

- Regular audits, which were executed by auditors of the Internal Audit Unit periodically (every second year, on average), probably would not have a strong possibility to identify all of the above irregularities, especially the following:

    - The misappropriation of cash derived from a customer's deposit account, which were taken by the fraudster employee without the customer's presence.
    - The forgery of customer's signatures on transaction documents and papers, especially if those documents have been initialized and the transactions have been authorized accordingly by the appropriate bank supervisors.
    - The poor control and monitoring of the daily work of the fraudster by his superiors.
    - The irregular money transfers between deposit accounts via web banking, which were made by using a pc located outside the bank, since they are untraceable.

- A Fraud Detection System was not in place, in order to detect internal and in collusion with external and collusive first party fraud by utilizing effective fraud scenarios and generating alerts and reports.

But, except of all the above mentioned, the most important thing for not detecting fraud at an early stage was the lapse of fraud awareness that applied to all of the bank's staff (clerks, supervisors, Branch or Unit Directors), since the company had not developed a relevant culture for detecting and reporting indications of internal fraud.

Red flags can indicate the possible need and/or opportunity to commit fraud. They must be considered within context; they are not absolute.

Red flags for internal fraud are:

Behavioral - Personal : an extravagant lifestyle (usually not aligned with personal and/or family profile); personality changes (negatively, complaining, becoming increasingly critical); a perceived/actual conflict of interest (e.g. approving mortgage loans that facilitate the sales of your father's broker company); a "breaking rules" attitude; a "controls are waste of time" attitude; a "management by fear" attitude; an arrogant or secretive nature; being afraid of losing job; financial pressures (medical bills, debts); personal-family problems (death, divorce, gambling, alcohol addiction etc.).

Task - related: Any financial transaction that does not make common or business sense; lack of dual controls procedures (4 eyes principal); control & access to customer's accounts & information, data and systems without adequate supervision; password sharing; inadequate separation of duties; conduct task with absolute trust of the supervisor; high employee turnover in vulnerable areas such as sales unit; compensation programs that are not taking risk into account.

3.2 Dealing with fraud cases (Key objectives, skills and responsibilities of people involved)

The most common incidents, which could cause a fraud investigation, are:

- Customers protest or complaint
- Prosecution of an employee by a customer

- Anonymous reporting for irregular or illegal actions taken by an employee
- Whistleblowing
- Audit findings indicating fraud, during a regular internal audit
- Press articles and publication, referring to fraud occurred in the company
- Information from other employees or third parties about an employee's behavior beyond his/hers normal and usual profile.

What to do when fraud is suspected?

Part of a good line of defense against fraud entails having a good offensive plan. Organizations should be prepared to act quickly when a suspected fraud is brought to their attention [8].

They should have an agreed upon set of protocols that address various scenarios. Below are some helpful suggestions that can guide an organization's response:

- Identify implicated parties
- Consider the quality of preliminary information
- Assess possible materiality of the allegation
- Be prepared to respond thoughtfully and consistently while recognizing that every matter is unique
- Consider the type and level of expertise necessary to investigate
- Consider logistics, such as timing and resources
- Consider the perspectives of others
- Investigate objectively
- Consider whether and when to engage the audit committee chair
- Report findings to appropriate stakeholders

It is essential for the management of an internal fraud case the full knowledge of the extent, of the persons involved in this and the known or potential risk, i.e. the kind of impact in the company.

For proper treatment and management of an internal fraud case, it is good practice to have in advance a relevant plan, as those for crises.

This plan should include key actions to be implemented in the context of the case management, as well as the persons, who will be involved in this in terms of business.

Given that, as mentioned above, there are various forms of fraud schemes, the company will have to make up a basic and flexible plan, with capability for adaptation to each specific case, since, as it is known, not all cases are the same and identical, because each one has several peculiarities and people, who are about to manage them, should be adequately prepared to face them aiming to positive results.

The key objectives of the business' responsible persons, who will deal with managing an internal fraud case, should be, indicatively:

- The immediate ending of the illegal activity of the fraudster employee and removal from his/hers position, in order to avoid continuing illegal actions and concealment or destruction of evidence.
- Thorough investigation of the case to identify the economic loss size and impact to the company.
- Limiting the economic damage by taking direct and immediate actions for recovery of lost business assets.
- The identification of persons (perpetrators, abettors and other parties involved in the fraud issue, within or outside the company), for accountability and prosecution purposes.
- Mitigating and reducing the negative impact of the internal fraud event for the company and its fame and market reputation.

The following questions arise:

- Who is qualified to manage an internal fraud case in a business?

- Who recommends measures to be taken, who decides and who execute decisions?

- How to deal with customers' complaints?

- How to preserve and protect the prestige and reputation of the company?

- How to mitigate the economic impact against the company by an event of internal fraud?

- How to ensure non-recurrence of similar incidents in the future?

Regarding the persons, who will undertake to manage an internal fraud case, they should definitely belong to the operational executives of the company, should have relevant experience and negotiation skills, good knowledge of the procedures of the area where the fraud occurred and have at their disposal adequate and permanent legal support.

These executives have to be informed about the findings of the investigation, which has been preceded, in order to know the events that led to fraud, the persons who committed the fraud, the type, extent and size of the fraud and its economic impact for the company.

For this purpose, they must cooperate with the investigators in all phases of the research, while examining ways of responses to suggest appropriately to senior executives of the company for decision making purposes about the company's attitude:

- To all customers who have suffered damage to their assets

- Against the employee, who committed fraud.

- Against the company's executives, who were responsible for monitoring the work of the fraudster.

Decisions are taken by executives, authorized accordingly by the General Management. In cases of large-scale fraud with large economic impact to the detriment of the company, decisions may be taken at BOD level.

Decisions should be implemented by the officers, who had taken over the management of the case, or by the relevant Business Units.

At all stages of this procedure, it is necessary for the assigned executives to cooperate with the legal department of the company.

The legal advisors of the company should inform these executives and the members of decision making Committees about the potential risks in each case and suggest ways of avoiding risks that could lead to lawsuits against the company.

Referring to the issue of handling complaints, protests and legal actions taken by company's customers, due to employee fraud, which adversely affected their savings or investment funds or their borrowing status or caused discredit, the treatment and management in terms of the company should be particularly careful.

The decision to compensate a customer should be taken after a consideration of the merits of the complaint and after it is ascertained that, indeed, there were malicious employee's actions against the client, without his knowledge or tolerance.

In any case though, it is very important, when deciding about compensation or satisfaction of a customer's request, to have in mind primarily protecting the reputation of the company and maintain the trust of its customers, issues which are essential for the continuity of the business.

Hence, in cases where it was found that client's tolerance in employee's irregularities and client's disregard for the management of his investments were the basis for the fraudster to commit fraud, the company decided to restore the loss of its customers, in order to gain their confidence and aiming to protect its reputation.

In internal fraud cases occurs, almost always, a direct economic impact to the detriment of the company, affecting the financial statements and profits, and possibly a medium-term economic impact, if the extent and type of fraud becomes broadly known and leads to loss of market share, implying turnover reduction and loss of revenues.

The recovery of financial loss arising from a customer's compensation is sought immediately and in every possible way, including auction of the fraudster's property.

Since the loss of confidence of customers and the loss of a market share, due to the disclosure of the fraud incident to the public, has absolutely a serious impact on a company, as it can lead to shrinkage of revenues and even a shutdown, companies attach great importance to how to deal with a case of fraud and seek in every way for withholding or degradation of its importance.

At the same time, of course, after the discovery of a case of internal fraud, it is important to reexamine the adequacy and effectiveness of internal controls and safeguards in operating procedures and regulations of the enterprise, to implement a new risk assessment and enhance check points and control procedures, in order to prevent recurrence of similar events in the future.

3.3 The role of the Internal Audit related to fraud

Internal auditors are in many respects the "eyes and ears" of an organization, responsible for evaluating the effectiveness of, and providing assurance on, the company's governance, risk management and internal control processes.

According to the International Standards for the Professional Practice of Internal Auditing, as promulgated globally by The IIA, as it relates to fraud internal auditors must:

- Have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. (Standard 1210.A2)

- Exercise due professional care by considering the probability of significant errors, fraud, or noncompliance. (Standard 1220.A1)

- (In its reporting), include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board. (Standard 2060)

- Evaluate the potential for the occurrence of fraud and how the organization manages fraud risk. (Standard 2120.A2)

- Consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives. (Standard 2210.A2)

- Accordingly, among other aspects as it relates to the risk of fraudulent financial reporting, internal audit's range of activities may include:

- Monitoring and evaluating results of whistleblower programs and collaborating with other departments to address results and remediate applicable findings
- Assessing compliance with the entity's code of ethics
- Conducting ethics surveys of employees
- Analyzing year-over-year changes in key metrics

In terms of treatment, investigation and management of internal fraud, it seems that the issue requires specialized knowledge and skills, and should be entrusted to qualified auditors [5, 9, 10, 11, 14].

Exploring internal fraud case is essentially a special audit, which has, compared with a regular internal audit, several peculiarities.

In order to achieve comprehensive and thorough investigation into the matter, which leads to the conduct of the special audit, the following audit steps are suggested:

- Assignment of special audit to a specialized auditor (preferably a Certified Fraud Examiner).

- Initial exploration of raw data and information in order to determine the scope of the audit, to assess the possible magnitude, extent and severity of the case and to obtain, where appropriate, any immediate action to reduce or recover the loss.

- Organize the audit procedure and scope.

- Cooperation between the assigned auditor and his supervisors at the Internal Audit Unit to address specific situations that arise throughout the special audit.

- Collection of the necessary evidence to support audit findings (hard copy or in electronic form).

- Archiving and safe custody of the evidence.

- Conducting interviews with persons, who participated or were involved in any way, directly or indirectly, in the case under investigation.

- Submission of relevant and specific questions and receiving in writing (preferably by hand) and duly signed personal opinions and/or explanations from each one of the above persons.

- Writing the special audit report [2].

  The preparation of the report is made by the special auditor.

  First, a brief description of the background of the case and the audit object is quoted.

  Audit findings follow, in a clear and concise manner, with references (for documentation) to the accompanying documents or written statements of the persons involved, where required. A fraudster's written confession, in details, is most preferable.

  After the exposition of the audit findings and the opinions of the perpetrator and other employees, auditor inputs his opinion based on the audit findings and the

written statements obtained and estimates of the total damage and economic loss.

Finally, responsibilities are allocated to the fraudster and other employees, for acts or omissions which resulted in financial loss or defamation of the entity, with clear reference to the rules and directives, which were not duly implemented or bypassed methodically.

- Reporting briefing notes before the completion of the audit.

  It is performed by the special auditor, when necessary, during the investigation, especially in cases of embezzlement against many customers. The purpose of this action is to quickly update the assigned persons, which are responsible for the management of each customer requests.

  Prior to the finalization of the special audit report, the auditor collaborates with the Legal department for particular legal advice.

The findings of the special audit, annexes and briefing notes must be signed by the auditor and delivered to the Internal Audit Unit, together with the accompanying documents and all kind of evidences.

The Internal Audit Unit executives review and finalize the special audit report, which is signed by the auditor and forwarded to the relevant executives, for information and action purposes [(9)].

For adequate and documented conducting of a special audit, auditors should:

- Be informed of the applicable procedures (Circulars, Regulations) relating to the matter under inquiry, before starting the special investigation.
- Cooperate with the employees (clerks, supervisors) of the auditee to obtain the required data and information.
- Have full and unrestricted access to obtain data from the company's information systems, when necessary.
- Maintain a record of the findings, by grouping the findings by subject and chronologically.
- Process and evaluate the findings and formulate a first aspect, in order to prepare questions that will be addressed to auditees and be prepared to refute the various excuses with citing compelling evidence.
- Address specific questions and seek to obtain clear, concrete and substantive responses, so they could not be susceptible to misinterpretation of the involved persons or the readers of the report.
- Keep chronology of events when recording audit findings.
- Avoid comments and references to sensitive personal data, other than those which are absolutely necessary for the documentation of audit opinion.
- Avoid comments and opinions, not proven and not documented.

- Make brief presentation (not a full copy) of written statements and explanations of persons involved in the case, with emphasis on the critical points, omitting minor references.

- Try to obtain, in cases of fraud, infidelity, embezzlement, forgery, written and detailed description of the methodology used by the liable employees, accompanied by a written statement of the reasons that led to it.

- Seek to obtain written confession and acceptance of liability and irregular - illegal - improper actions from fraudsters.

- Assess the audit findings and written statements obtained when expressing audit opinion.

- In cases of non-compliance or deviation from Circulars and directives, refer specifically to them (number and theme of Circular, specific provision found unobserved).

- Not address liabilities not arising from the audit findings or not clearly documented.

- Not consider the views of the auditees as evidence of accountability, if not substantiated by the audit findings.

- Treat each fraud case accordingly, bearing in mind that the conclusions of the investigation or even the audit report itself may be submitted to a court of justice or a Prosecutor, in order to support the company's positions. Therefore, the conclusion must be drawn in such a way as to be easily readable by people without specialized knowledge (e.g. prosecutors, judges).

- Keep all report drafts and notes in their archives and not destroy them, without prior consultation with their supervisors, since this information could be useful after several years, when the case would be at the judicial investigation stage or an ongoing trial and they could appear to testify as witnesses before a Court or Prosecutor.

- Propose corrective measures and improvement of existing procedures where appropriate.

The special audit should be treated by auditors with due seriousness and responsibility, regardless of its objective.

If the above suggestions are being followed by all auditors, then:

- Audit reports will be comprehensive and documented.

- Not much time will be needed for overviewing and finalizing the audit reports.

- The General Management and the appropriate Committees will have adequate information without delay.

- Decisions will be taken immediately.

- Audit findings will be evaluated and, when needed, corrective actions will be implemented.

3.4 Examples of internal fraud cases

Case A: Internal Fraud in business financing procedures

The case

During a regular internal audit in businesses' files financing documents at a Bank Branch, auditor found some credit limits approvals to customers without following the Bank's credit procedures and not according with standard and objective funding criteria.

Specifically, it was found that:

- The Branch's Credit Committee had approved credit lines to several customers for business loans over the general credit limit available for the particular Branch and, in many cases, without adequate guarantees.

- Most of these enterprises, despite that they were newly established and had zero turnover, were funded with hundreds of thousands Euros, in terms of working capital.

- For some of those business loans the Branch had accepted as collateral, securities (postdated checks), which did not come from a commercial activity, but in fact, as it was ascertained by the auditor, they were issued just to deceive any potential audit, since their existence in the Bank's files meant that the related loans were sufficiently secured.

All these credit facilities had been approved by the Committee members (Branch Manager and Deputy Manager), who knew from the very beginning that, by those credit approvals, they were exposing the bank to a large credit risk.

A few days after the first audit findings which were pointing out that something was going wrong with the specific loans, the Deputy Branch Manager told the auditor that he was resigning and left immediately the Bank, taking with him many of the postdates checks, which were supposed to secure the loans.

After that, the auditor informed the Director of the Internal Audit Unit and the case was assigned to a special investigator of the bank, for further in-depth investigation of the issue, conducting interviews, collecting evidence and reporting the relevant findings.

The Deputy Manager was not found to give explanations to the auditor for his actions.

During the investigation it was revealed that many companies did not exist at all, nor had there ever been (they had provided the bank with nonexistent address or residential addresses of individuals or other business).

During the interviews, conducted by the auditor, many employees of the Branch submitted in writing that in the case of the above mentioned financing approval process a third person was involved, too, who had a personal relationship and friendship with the Deputy Manager and the two of them worked together to defraud the Bank.

Employees testified that they had seen several times this third person visiting the bank and delivering data and documents of alleged enterprises, which the Deputy Manager was taking and, based on these, he filled their written requests for financing and subsequently approved them along with the Manager.

After the approval, the supposed businessmen were visiting the Branch, to sign the financing contracts and transaction forms for withdrawals from the loan accounts, which were giving to the Deputy Manager and, after that, they did not appear again in the bank.

Also, the Branch cashiers, when the auditor asked them, revealed that the Deputy Manager, taking advantage of his position in the bank, had given them orders to execute withdrawal transactions from the loan accounts, using the relevant documents, which were already signed by the alleged debtors and he himself was taking the money in cash, which he was delivering afterwards to his friend, inside or outside the bank's premises.

Auditor found, also, that a significant amount of money had been deposited, partially during the last two years, in the Manager's current account.

When the Manager was asked by the auditor about the origin of this money, he initially tried to mislead him, claiming that the money was given from a relative of his, to deposit it in his account, but in the end he admitted that this money was his share for concealing the fraudulent actions of the Deputy Manager and his friend.

The management of the case, after the disclosure of fraud

The particular fraud case had a serious economic impact on the bank, since it was revealed that several million euro loans had been given to non-creditworthy borrowers, without collaterals.

The report of the special investigation was delivered by the auditors to the Internal Audit Unit and circulated immediately to specific Units and executives of the Bank, who acted as follows:

- **Human Resources Unit:**
  The Manager and the Deputy Manager of the Branch were fired immediately.

  The dismissal of these officials and the reasons behind this, were not made known widely to other customers, in order to avoid defamation of the bank.

  The bank also imposed disciplinary sanctions to cashiers because they executed transactions without the customers' presence, using pre-signed documents and hand over cash sums to the Deputy Manager, for whom they knew that then he was delivering the cash to his friend, but they had never mentioned something about these ongoing irregular and improper actions to a superior officer of the bank to reveal the fraud early.

  These disciplinary sanctions were communicated to the bank staff with internal circular (without reference in persons and names) to be an example to be avoided and to indicate to staff the negative consequences encountered by those, who are engaged in such actions.

- **Legal Advisors Unit:**

  Efforts were made to find assets in the name of alleged debtors.
  Most of the borrowers did not have any significant asset and the bank just filed lawsuits against them (for some of them, in the names of whose properties were found, the bank proceeded in auctions).

The cases of lawsuits are still pending but, even if the suited persons were sentenced in the criminal courts and brought to jail, that does not mean that the bank will gain something out of it, in terms of economic loss recovery.

The bank also filed a lawsuit for fraud, claiming compensations, against the ex – employees (Manager and Deputy Manager) and against the Deputy Manager's friend, who according to the testimony of other employees of the Branch, was taking the cash from loans.

The bank's lawsuit and claim against its ex- executives became known to all Personnel by internal circular of the HR Unit (without reference in names and persons) for preventing fraud purposes.

- **Operational Supervising Units:**

The borrowers were invited by officers of the supervising Regional Branch Unit, who were assigned to manage the case, at the bank's Head Office and were informed that there would be legal actions against them, given that they had signed the contractual documents and transaction documents for taking cash of the relevant loan accounts, regardless if in fact they had received or not the loans.

Meanwhile, the Regional Branch Unit gave appropriate instructions to employees of the Branch, of how to answer customers' questions about where did the two former executives go so suddenly (they were instructed to reply that the Manager retired and the Deputy Manager resigned, because he wanted to deal with his personal business).

Thereby the bank's defamation was avoided and there was no loss of customers or decrease of deposits and credit loans of the Branch.

- **Accounting treatment:**

The money found during the audit in a Manager's current account, as derived from criminal activity, were used by the bank to recover its losses.

The majority of the loans were written off from the GL bank accounts.

This decision was made by a special Committee, which had been set up in the bank to manage operational risk events, after the completion of the special audit and legal actions, since there were no assets to liquidate in order to recover some amount.

The write-off of the above loans affected negatively the economic size and the financial results of this Branch (and the Bank, respectively, to a lesser extent) and it took a long time to be replaced with new credit facility limits approvals.

Also, the above significant reduction of the economic size resulted in the Branch's degradation in a lower position (an internal process of the bank, that evaluates and classifies its branches under aggregates and balances, per year), which had a negative impact on salaries and extra benefits (bonuses) of the Branch's executives.

- **Strengthening controls - Update and review of procedures:**

This fraud case has prompted a reviewing of the funding approval process and a few months after the Bank decided to abolish the Branches' ability of approving credit facilities.

Also, internal instructions for the proper execution of transactions were reminded to the Branch network, transactions without the customer's presence and use of pre-signed documents were explicitly banned and staff was encouraged to report

suspicious events and behaviors of other employees, by introducing a confidential line of anonymous reporting.

Case B: Internal fraud in investment products

The case

An investment company officer (investment advisor) responsible for managing the investment portfolios of wealthy customers, taking advantage of the customers' trust, was suggesting them to invest their money in floating rate notes (FRN), without informing them of the nature of this particular investment product and the risks of this kind of investment.

The reason that this particular officer made such suggestions to his clients was, basically, to achieve all of his goals set by his superiors, so that to get, at the end of the year, a big bonus from his company.

Since these investment products were of high risk and their odds evolved negatively, with negative impact on the customers' invested capital, customers began to protest and expressed their will of withdrawing their money.

The investment advisor, fearing that, if the customers materialized their will, this could affect negatively his personal life (less or not at all bonuses, loss of his job), decided to mislead and conceive them.

In order to do so, he informed the customers that he was intending to transfer their funds to safe and low – risk investments, such as mutual funds and term deposits and persuaded them by manufacturing and delivering to them, as a proof of their investment, fake documents, which were copies of original ones processed by him in such way that they seemed original.

In those forged documents he had recorded virtual amounts and interest rates along with falsified signatures of existing bank officers, so the customers were convinced that their money was invested in these products and stopped protesting.

The investment advisor also managed to alter the customers' mailing addresses, by entering in the company's information systems as a new address of each customer the address of the investment company's premises.

By this action, customers received no longer information about the monthly updated status and balance of their portfolio (he himself received, instead of them, all relevant correspondence) and they could not know his investment movements using their money.

If a customer called him, giving the order to liquidate his investment, the investment advisor was calculating the exact amount (invested capital plus interest) that should be granted to the customer based on the forged document he had provided him before and, after that, he was giving order to liquidate existing term deposits of other clients (which he was aware of, since he managed many clients' investment portfolios), without their knowledge and consensus and transferred, with new orders, those amounts to the first customer's account.

The ordinary procedure followed at the investment company, in investment portfolio liquidation cases, was:

1) Customer order for investment liquidation, transmitted via telephone to the investment advisor.
2) Investment advisor order to the collaborator Bank, through internal on – line connection between the investment company and the Bank.

3) Liquidation transactions processed by the Bank, resulting to money transfer to the ordering client's current account.
4) On-line information provided for the investment advisor at every stage of the above process.

Once the investment advisor saw on his personal computer screen that the order had been executed, he was sending a new transaction order to the Bank, following the internal on-line process, to transfer the amount from the customer's account to the account of the first customer, who wanted to liquidate his investment and then he was informing him via telephone that his money was available in his account.

The investment advisor's activity was revealed accidentally, when a client went at a Bank's branch bearing a forged document as proof of his term deposit and asked the cashier to liquidate it, without first informing the investment advisor.

The bank's cashier recognized that the presented document was forged, informed immediately his superiors and then told the customer that he could not pay him, since the document was not authentic.

The client protested strongly and threatened to take legal action against the bank and the investment company.

Since the issue had indications of fraud, the investigation of the case was assigned to a special investigator of the Bank's relevant department at its Internal Audit Unit, in cooperation with the Internal Auditor of the investment company, which was a Bank's subsidiary.

The two auditors did not exceed their investigation up to the complaint of the specific client, but they extended it to the investment portfolios of all clients, who had been collaborating with the particular investment advisor in the past.

During this investigation it was ascertained that the advisor's fraudulent activity had affected the portfolios of many customers, but also another fraud issue was revealed, in which the same investment advisor was involved.

Specifically, it was found that the advisor had managed, during a two year time, to withdraw a large amount from the customer's deposit account, using blank transaction documents already signed by the account holder.

The advisor had persuaded the customer to sign many blank transaction documents by telling him that, by this way, he could execute transactions on behalf of him, without being necessary for him (the customer) to be present every time at the Bank, whenever he needed to withdraw money from his current account.

Those pre - signed documents had been presented by the advisor at the Bank's cashiers, who already knew him and trusted him and never suspected that he was acting for his own benefit.

As a result of the above the cashiers, following his instructions, executed withdrawal transactions on the customer's account, without the customer's presence or written orders, bypassing the Bank's relevant procedure and regulations and paid the advisor in cash.

The investment advisor, exploiting the customer's confidence and trust and knowing that he was not checking at all his current account and its balance, withdrew illegally large amounts of money and consumed them in luxurious restaurants and clubs, expensive clothes, jewelry, gambling and other kinds of entertainment.

<u>The management of the case, after the disclosure of fraud</u>

The report of the special investigation was delivered by the auditors to the Internal Audit Unit and circulated immediately to specific Units and executives of the Bank and the Investment Company.

The management of the case involved members of the following Units, who acted specifically:

- **Human Resources Unit:**

  The fraudster investment advisor was fired immediately.

  The bank imposed disciplinary sanctions to the cashiers, because they executed transactions non complying with the bank's regulations, without the presence of the client, using pre – signed transaction documents and paid in cash the investment advisor, actions which resulted in not disclosing the fraud.

  These disciplinary sanctions were communicated to the bank's staff by an internal circular (without reference to names of employees) as an example of actions to be avoided and to indicate the negative consequences encountered by those who are engaged in such actions.

- **Legal Advisors Unit:**

  An immediately research for possible existence of assets and property in the name of the fraudster was conducted and the company managed to engage it with mortgage, so as to be able to proceed to auctions, in order to limit the economic damage.

  The Investment Company and the Bank filed a lawsuit against the fraudster for fraud, forgery and embezzlement, and claimed reimbursement of all economic damages.

- **Operational Supervising Units:**

  Senior executives of the company looked for all customers, whose investment portfolios were managed by the investment advisor and asked them to visit, one at a time, the company's head office, providing any kind of evidence they might have had for their investments.

  For those customers, who were found to possess counterfeit evidence of deposit, when in fact they had, without knowing it, only high-risk corporate bonds, since the negotiating efforts of the company's executives had no effect, it was decided to liquidate existing corporate bonds and then to reimburse customers, in cash, with the value of the false evidence of deposits they possessed, covering the reimbursements with company's funds.

  The above decision was taken by the General Manager of the company, in order to prevent any protests and actions against the company, which would result in defamation of the company and would probably lead other customers to withdraw their funds, something that was avoided in the end.

  Also, the company decided to restore in full, plus interest, all customers' term deposits, which had been liquidated without their knowledge by the fraudster to cover capital losses of other clients from investments he had suggested in high risk products.

  As for the client, from whom the fraudster embezzled a large sum of money, using pre- signed documents, the bank assigned the management of the case to the Head of Branch Supervising Unit (Regional Director) in cooperation with the legal advisors of the bank.

  Following discussions and negotiations between the bank's executives and the client's lawyer it was finally decided to make an extra- judicial settlement and the bank returned a 50% of the money, since the client admitted his own responsibility, because he had signed numerous white transaction documents and had given them to the investment advisor for money withdrawal purposes

and, in the meantime, he had never checked his current account status and balance.

The decision for this kind of settlement was recommended by the Regional Director, who handled the case, was taken by the specific Operational Risk Management Committee and was beneficial to the bank, since the initial customer's claim was reduced to 50%, while there was a serious risk that, if the case was appeared to court, the bank could lose the case and be sentenced to pay back 100% of the money misappropriated, plus interest.

- **Accounting treatment:**

  After immediate actions taken by the company's lawyers, the fraudster's property was divested by auction and the company received an amount, which was used to reduce the economic damage suffered by compensating customers.

  The remaining amount from the customers' compensation, which was not covered by the liquidation of the property of the fraudster, burdened the economic results (profits) of the company, by decision of the Operational Risk Management Committee.

  Also, by decision of the respective Committee of the Bank, the amount paid as compensation to the client, from whom the fraudster had withdrawn illegally funds from his account, burdened the economic results (profits) of the bank.

- **Strengthening controls - Update and review of procedures:**

  This case was an occasion for reviewing and redesigning processes, involving:

  - The ability to change customer's correspondence data in the information system of the investment company.
  - Alternative ways for customer information and verification of transactions executed, which affected the current status of their investments (e-mail, SMS, etc.).
  - Development of dual control (four eyes principle) for the completion of an investment transaction.

  Also, the Bank reminded its Branch network of the existing internal rules and regulations for the proper execution of transactions on client accounts (physical presence of the account holder, who should sign the transaction document in front of the cashier or written authorization to a third person, which previously should have been checked and approved by the cashier's supervisor).

3. Conclusions

A well-organized internal control system, with adequate security safeguards and checkpoints, segregation of duties, double checks (four eyes principle) at various stages of the procedures, information system providing, through data processing, alerts of possible fraud, an adequately resourced Internal Audit function are necessary elements in a business, to prevent or timely disclose fraud phenomena.

It is very important for the General Management of the business to have the sensitivity for fraud prevention (tone at the top), which by all means should be communicated to the staff of the company.

Internal fraud incidents in a business are, of course, undesirable, but they cannot be excluded, despite the efforts to prevent them, based on the above described actions, procedures, regulations and business policy, in general, against fraud.

The results of an internal fraud have an impact primarily on revenue and reputation of the company and, depending on the size of the fraud and its publicity, may lead to the closure of the business.

It is therefore very important and necessary to have prior a business plan for immediate treatment and proper management of internal fraud cases, to minimize the negative effects and, especially, to protect the reputation and brand name of the entity, so to be able to overcome soon, by the continuation of its business activity, any negative economic impact caused from the fraud event.

Persons with appropriate skills should be assigned to implement an internal fraud management plan.

Those persons should be working for the company and be empowered to suggest or decide actions on behalf of the company.

To successfully manage internal fraud and minimize the impact to the detriment of the business, there should be adequate and accurate information of the assigned people on the details of the case and an estimation of financial loss.

This information should be provided through a special audit performed by a qualified auditor of the Internal Audit Unit, in order to investigate in depth the internal fraud case.

Internal Audit investigates the fraud case and delivers the audit report, but is not involved in submitting suggestions and make decisions process (a representative of the Internal Audit Unit may attend relevant Councils and Committees, in an advisory role) nor participates in meetings and negotiations with clients while managing the internal fraud cases.

The investigation of a fraud case has, also, some other objectives, related to the internal operation of the business.

Based on the special audit's findings, the competent Units/Departments of the firm:

- Assign responsibilities and impose disciplinary sanctions against employees, who actively participated in the fraud case or facilitated, by their actions or omissions, the fraud and its concealment.

- Identify gaps and failures in process control points, which the fraudster took advantage of to achieve his illegal purpose without disclosing his actions.

- Strengthen the safeguards and review - modify - improve existing regulations and internal procedures.

Companies should have, as a priority, actions that contribute to information and awareness of their employees in matters of fraud, since "Prevention is better than Repression".

4. Bibliography

1. ACFE 2018 Fraud Examiners Manual, International Edition. Association of Certified Fraud Examiners, Inc. 2018
2. ACFE Research Team. Report Writing Manual. Association of Certified Fraud Examiners, Inc. 2018
3. ACFE Report to the Nations on Occupational Fraud and Abuse 2018 Global Fraud Study. Association of Certified Fraud Examiners, Inc. 2018
4. ACFE, AIPCA and The IIA. Managing the Business Risk of Fraud: A Practical Guide. Association of Certified Fraud Examiners, Inc.2011
5. Albrecht, Steve W- Albrecht, Chad- Wells, Joseph T. Fraud Examination & Prevention. Thomson South-Western, 2003.
6. COSO, ACFE. Fraud Risk Management Guide. 2016
7. Cressey, Donald R. Other People's Money: A Study in the Social Psychology of Embezzlement. Montclair, N.J.: Patterson Smith, 1973
8. Lackstrom, Carl. Preparing for Fraud: Performing Fraud Response Planning. RSM McGladrey Inc., November, 2006.
9. Pednault, Stephen. Anatomy of a Fraud Investigation: From Detection to Prosecution. John Wiley & sons Publishing, 2010
10. Petrucelli, Joseph R. Detecting Fraud in Organizations. John Wiley & sons Publishing, 2013
11. Sutherland, Edwin H. and Cressey, Donald. Principles of Criminology. 11th ed. Lanham, Md.: AltaMira Press, 1992.
12. Vona, Leonard W. Fraud Risk Assessment: Building a Fraud Audit Program. John Wiley & sons Publishing, 2008
13. Wells, Joseph T. Principles of Fraud Examination.4th edition. Wiley 2017

Other bibliography

Askelson, Ken, et. al. Global Technology Audit Guide 13: Fraud Prevention and Detection in an Automated World. The Institute of Internal Auditors, 2009. http://www.theiia.org/bookstore/product/global-technology-audit-guidegtag-13-fraud-prevention-and-detection-in-an-automated-world-download-pdf-1464.cfm

Anti-Fraud Collaboration. Closing the Expectation Gap in Deterring and Detecting Financial Statement Fraud: A Roundtable Summary. 2013. https://na.theiia.org/standards-guidance/Public%20Documents/Anti-Fraud%20Collaboration%20Report.pdf

Anti-Fraud Collaboration. How to Improve Your Whistleblower Program and Address Impediments to Reporting. Webcast originally aired July 1, 2014. http://antifraudcollaboration.org/

http://www.Banktech.com article # 1318489 - How Fraud & Cyber Security Will Evolve in 2015 article # 1318447 - Plan Ahead for Financial Institution Fraud Management in 2015

Bart, David P. and Scott Peltz. “The Threat Within: Employee Fraud Detection and Prevention.” McGladrey.com. http://mcgladrey.com/content/dam/mcgladrey/pdf/threat_within_employeefraud_detection_prevention.pdf

Basilico, Elisabetta and Hugh Grove. “Major Financial Reporting Frauds of the 21st Century: Corporate Governance and Risk Lessons Learned.” Journal of Forensic & Investigative Accounting 3, no. 2 (2011): 191 -226. http://www.bus.lsu.edu/accounting/faculty/lcrumbley/jfia/Articles/FullText/2011_v3n2a7.pdf

BDO Consulting. Doing Business Abroad: Spotlight on UK Bribery Act. BDO, 2011.
BDO Seidman, LLP. The BDO Consulting Critical Anti-Fraud Program Creating; A Genuine Anti-Fraud Environment. BDO, 2008.
http://www.bdoconsulting.com/resources/brochures/BC-CAPbrochure5-08.pdf

Brazel, Joseph, Keith Jones, and Mark Zimbelman. Using Nonfinancial Measures to Assess Fraud Risk. The IIA, 2008.

http://www.theiia.org/bookstore/product/using-nonfi nancial-measures-to-assess-fraud-risk-1374.cfm

Carpenter, Tina and Jane L. Reimers. "Professional Skepticism: The Effects of a Partner's Influence and the Presence of Fraud on Auditors' Fraud Judgments and Actions." SSRN, September 1, 2009.

http://ssrn.com/abstract=1068942

Center for Audit Quality. Deterring and Detecting Financial Reporting Fraud: A Platform for Action. 2010.

http://www.thecaq.org/docs/reports-and-publications/deterring-and-detecting-financial-reporting-fraud-a-platformfor-action.pdf?sfvrsn=0

https://charteredaccountantsanz.com Fraud and corruption trends for 2015 (Feb 2015)

Flood, Brian. "Addressing the Risks of Fraud and Misconduct." (Presentation at the Internal Auditor's Association Conference, Austin, TX, December 1, 2010.)

KPMG. Who is The Typical Fraudster. KPMG LLP, 2011.
http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/who-is-the-typical-fraudster.pdf

Kroll, et. al. 2013/2014 Global Fraud Report. New York: Kroll, 2013.
http://fraud.kroll.com/wp-content/uploads/2013/10/GlobalFraudReport_2013-14_WEB.pdf

McNeal, Andi. "The Role of the Board in Fraud Risk Management." The Conference Board Inc., January, 2011. doi: DN-V3N21-11. http://www.conference-board.org/retrievefile.cfm?Filename=TCB-DN-V3N21-111.pdf&type=subsite

NACD and the Anti-Fraud Collaboration. Skepticism Series to Combat Fraud. October 1, 2012, and continuing.
http://www.nacdonline.org/Education/skepticismwebinars.cfm?navItemNumber=3717

Pergola, Carl W. "Simplicity in the Face of Complexity: An Integrated Approach to Anti-Corruption Initiatives." ViewPoints, no. 1 (2011): 2-3.
http://www.bdoconsulting.com/resources/publications/BDOC-Viewpoints-2011-Issue%201%20Newsletter.pdf

Public Company Accounting Oversight Board. "Consideration of Fraud in a Financial Statement Audit." SAS No. 1, Section 316 (2002).
http://pcaobus.org/standards/auditing/pages/au316.aspx

PwC. Confronting Corruption: The Business Case for an Effective Anti-Corruption Program. PricewaterhouseCoopers LLP, 2008.
http://www.pwc.com/en_TH/th/publications/assets/confronting_corruption_printers.pdf

PwC. Cybercrime: Protecting Against the Growing Threat. PricewaterhouseCoopers LLP, 2011. http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf

PwC. Fighting Economic Crime in the Financial Services Sector. PricewaterhouseCoopers LLP, 2011. http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/fighting-economic-crime-in-the-financial-services-sector.pdf

Rollins, John. Addressing Financial Fraud in the Private Equity Industry. McGladrey LLP, 2014. http://mcgladrey.com/content/dam/mcgladrey/pdf_download/wp_fas_addressing_financial_fraud.pdf

Schilit, Howard M. "Financial Shenanigans: Detecting Accounting Gimmicks that Destroy Investments." CFA Institute Conference Proceedings Quarterly 27. no. 4 (2010): 67-74. http://www.cfainstitute.org/learning/products/publications/cp/Pages/cp.v27.n4.1.aspx

Stippich, Warren and Mark Sullivan. "Fraud in the Economic Recovery." CorporateGovernor, Spring, 2010. http://www.grantthornton.com/staticfiles/GTCom/Advisory/Advisory%20publications/Corporate%20governance/CGwhitepaper.pdf

The IIA. "Al Hands on Deck: Partnering to Fight Fraud." Tone at the Top, no. 65 (2013). https://na.theiia.org/periodicals/Public%20Documents/TaT_December_2013.pdf

The IIA. International Professional Practices Framework (IPPF). The IIA Research Foundation, 2013. http://www.theiia.org/bookstore/product/international-professional-practice-framework-2011-1533.cfm

The IIA. "Practice Advisory 1210.A2-2: Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution, and Communication." NJ IIA, last modified April 27, 2006. http://www.njiia.org/training_items/Practice_Advisory_1210[1].A2-2_Rev_4_27_2006.pdf

The IIA. International Standards for the Professional Practice of Internal Auditing (Standards). The Institute of Internal Auditors, 2012. https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

The IIA. The Three Lines of Defense in Effective Risk Management Control. The Institute of Internal Auditors, 2013. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

The IIA. "Practice Advisory 1210. A2-1: Auditor's Responsibilities Risk to Fraud Risk Assessment, Prevention, and Detection." Njiia.org

http://www.njiia.org/training_items/Practice_Advisory_1210[1].A2-1_rev_4_27_2006.pdf