Department of Economics

Faculty of Economics and Political Sciences

National and Kapodistrian University of Athens

MASTER IN BUSINESS ADMINISTRATION

Direction: INTERNAL AUDIT

Title of Thesis:

COSO and ACFE fraud risk management guide. A research on how an organization can implement it in practice.

Writer: APOSTOLOS CHRYSOSTOMIDIS

Communication data:

E-mail: achrys8@hotmail.com
Mobile Phone: 00306948515120

Supervisor: Ass. Professor Dimitris Kenourgios

Supervisory committee members:

Professor Panayiotis Alexakis
Mrs. Evaggelia Dimitroulia

Date and place: November 2018, Athens

"I declare that I am the author of this thesis and that any assistance (data, ideas) which I received in order to prepare it, is fully recognized and is referred in the thesis. I even declare that this thesis was prepared personally and exclusively by me and I shall fully accept the consequences if it is proved that this thesis is not mine. Furthermore, I understand the University's rules on academic dishonesty and plagiarism and I am aware of the consequences which may follow if I breach those rules".

Tale of contents

Abstract

The study examines the adoption by Greek companies of the COSO - IC-IF (Committee of Sponsoring Organizations of the Treadway Commission- Internal Control –Integrated framework) and specifically its Principle 8, which states that "The organization considers the potential for fraud in assessing risks to the achievement of objectives". Furthermore, Fraud Risk Management Guide (2016) that includes five principles consistent with the five COSO Internal Control Components and the 17 COSO principles methodology is reviewed for organizations desiring to establish a more comprehensive approach to managing fraud risk, this guide includes more than just the information needed to perform a fraud risk assessment.

The study examines and analyzes the way Greek organizations consider the risk of fraud as a mean of prevention and detection as well as an ongoing, comprehensive Fraud Risk Management process.

In terms of methodology, 15 executives were selected as a representative sample and were interviewed. The interviews were based on a customized set of questions through which conclusions were drawn and opinions were exported on how organizations examine and manage the risk of fraud.

The research highlighted that fraud is affected by the organizational structure, Corporate Governance and not being familiarized with the concept of FRM.

Disclaimer: It has to be noted that all interviewees represent Greek entities that are subject to the Greek territory and legal status.

Because opinions and data are quite sensitive, the principle of confidentiality and non-disclosure have been adopted and followed. Thus, the names of the examined organizations and interviewees were not included in the research.

Furthermore, the aforementioned questionnaire does not contain personal data but does contain useful opinions of some experts who are involved in Fraud Risk Management.

CHAPTER 1: Introduction

The main objective of undertaking the current study was to identify the Greek reality about how organizations assess and manage the risk of fraud.

Interviews were conducted instead of questionnaires, since they provide more direct and honest answers. Interviews enable the connection between the interviewer and the interviewee in a more emotional basis than the fill of a typical questionnaire. The questionnaire is impersonal and anonymous, removing the risk of not answering openly, especially in sensitive areas like fraud. The interview includes communication, sharing, watching the body language etc. It helps to perceive when the interviewee prevaricates, when they avoid telling the truth, and thus the conclusion is deduced in a different manner than if it was conducted via a questionnaire on an electronic platform.

Moreover, external auditors from big auditing companies were interviewed, in order to get insights from another aspect regarding the way organizations react in fraud prevention and detection as well as in the overall management of fraud.

In the research, 15 Greek executives have participated and answered 26 open and closed questions. Additionally, 6 Chartered accountants were also interviewed and answered to 10 questions.

The research showed that fraud is associated with the organizational structure, as large sized organizations are more familiar with FRM. In addition a weak Corporate Governance weakens all actions towards FRM.

The thesis consists of four (4) chapters. The first chapter includes the purpose of the research, the methodology followed and the structure of the thesis. The second chapter includes the literature review where the COSO IC-IF is analyzed. In addition, the concepts of FRM as well as 2018 Report to the Nations are examined. The third chapter presents the methodology of the research and statistical data deduced from the interviews. Finally, the forth chapter outlines the main conclusions of the research as well as critically asserts recommendations for further research.

I would like to thank all named and anonymous participants who contributed with their expertise and knowledge in completing my research. I hope this survey will be useful to any related reader as it can affect many organizations to reexamine the way they manage fraud risk.

CHAPTER 2: Analysis of the theoretical foundation of the study

History of Internal Control framework

COSO (**Co**mmittee **o**f **S**ponsoring **O**rganizations of the Treadway Commission) is a joint initiative of five sponsoring organizations headquartered in the United States:

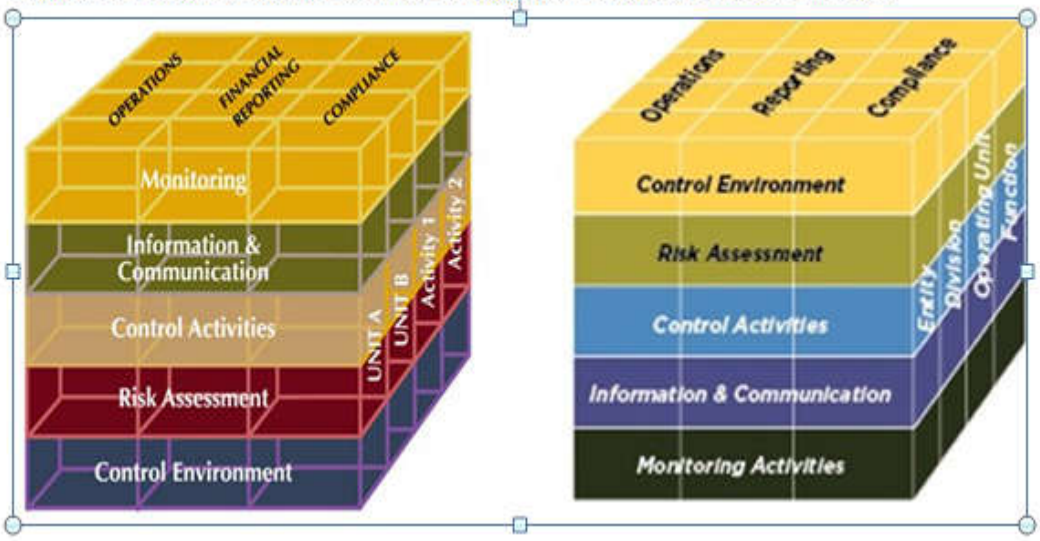
- the American Accounting Association (AAA)
- the American Institute of Certified Public Accountants (AICPA)
- the Financial Executives International (FEI)
- the Institute of Management Accountants (IMA)
- the Institute of Internal Auditors (IIA)

COSO was established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting,
COSO's main goal is to provide a direction to each concerned party by dealing with three interrelated subjects:

- ERM,
- Internal control and
- Fraud

COSO's first release was **Internal Control –Integrated framework (IC-IF)** in 1992. In May 2013, COSO issued a revised and improved edition of **Internal Control – Integrated framework**. One of the main purposes of this new framework was to prevent and detect fraud. Regarding objectives, financial reporting was replaced by Reporting which means internal and external, financial and non-financial reporting. Another critical change was a step by step approach to enhance its 5 components by developing of the 17 relative codified principles, supported by 87 detailed point of focus that may guide organizations to conduct a gap analysis between current and ideal condition through a maturity model structure.

Figure 1: COSO Internal Control–Integrated Framework 1992 vs 2013



Source:https://www.google.gr/search?q=coso+1992+vs+2013&client=firefox-b&dcr=0&tbm=isch&source=iu&ictx=1&fir=A9-G3-rVHhpwzM%253A%252CpK1dm-MCYFN7ZM%252C_&usg=__6IkkOst3VJyXvvWafQSdJb_s_B0%3D&sa=X&ved=0ahUKEwiP3fy

In September 2004 through the contribution of PricewaterhouseCoopers, COSO issued Enterprise Risk Management-Integrated Framework (COSO ERM), which main target was not to replace COSO IC-IF, but rather to enhance the internal control framework by focusing more and expanding to Enterprise Risk Management.

An updated version of COSO ERM retitled as Enterprise Risk Management—Integrating with Strategy and Performance was issued in September 2017. This publication concerns an attempt to identify new risks as they evolved and changed the last decade and also to present how they are managed.

Apart from ERM and Internal Control, the 3rd subject of COSO is fraud. There are many definitions of fraud but one has set by the "Practical guide managing the Business Risk of fraud", which defines fraud as an intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain (2008).

In July 2002 as a reaction to a number of major financial statement fraud, like Enron, Tyco International plc and WorldCom, enacted by United States Congress, the Sarbanes-Oxley Act (SOX), which set a number of requirements for all U.S. public companies in order to protect investors from fraudulent accounting activities by corporations. The most important key provision is Section 404, which states that

management install internal controls and both management and auditors develop reporting methods for the design and effectiveness of these controls.

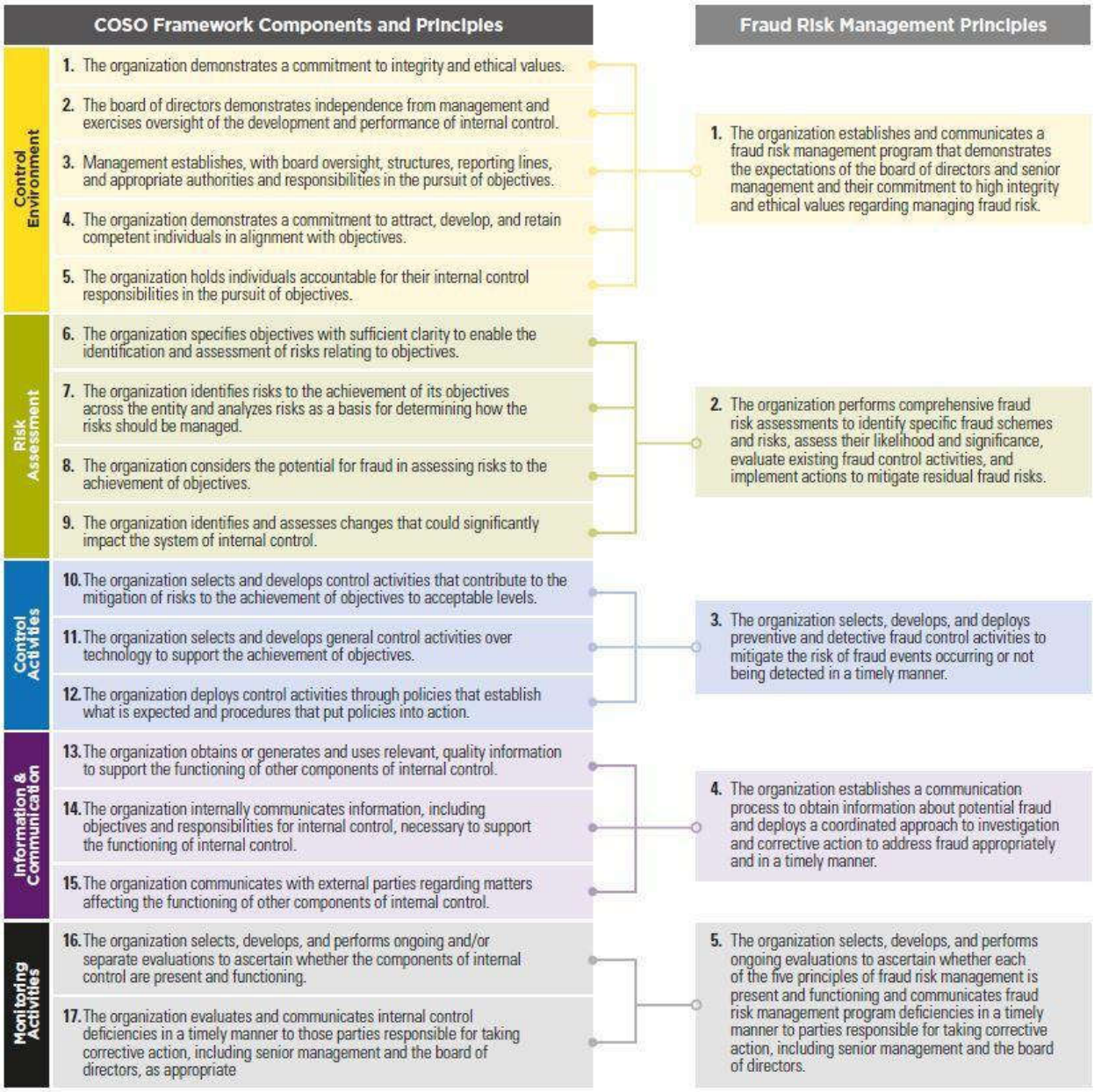
In 2008, a practical guide "Managing the business risk of fraud" was issued, sponsored by the IIA, AICPA and ACFE. This manual is focused on five Principles that help organizations to understand and manage fraud.

In 2018 ACFE has been issued **the 2018 edition of the Report to the nations,** a report of a great value that provides useful information for all fraud examiners and practitioners, government officials and any other interested in occupational fraud and abuse globally.

Moreover, in 2016 COSO and ACFE, based on the 2013 IC –IF, issued the **Fraud Risk Management (FRM) guide** a useful tool for managing fraud risks. This guide is an updated and complementary edition of "Managing the business risk of fraud: A practical guide", which helps organizations to establish a FRM program. We notice that in this guide the word "fraud" appeared 2.862 times per 148 pages document, whereas in 1992 COSO appeared 12 times per 139 pages document and in 2004 ERM 12 times per 139 pages document, demonstrating the great importance of fraud in the enterprise risk and control framework.

FRM guide connects FRM principles with the 2013 COSO Framework's five Components and 17 Internal Control Principles as follows:

Figure 2: Relationship between the 2013 COSO framework's 5 components and 17 internal control principles and FRM guide 5 principles.



Source:*https://www.ey.com/Publication/vwLUAssets/ey-effective-implementation-of-coso-thought-leadership/$FILE/ey-effective-implementation-of-coso-thought-leadership.pdf*

FRM guide states that operational risk apart from fraud includes risk associated with errors and unintentional omissions. The essential difference between error and fraud is the intention. Thus, there is a fundamental difference between internal control deficiencies ending up in errors than deficiencies ending up in fraud (2016).

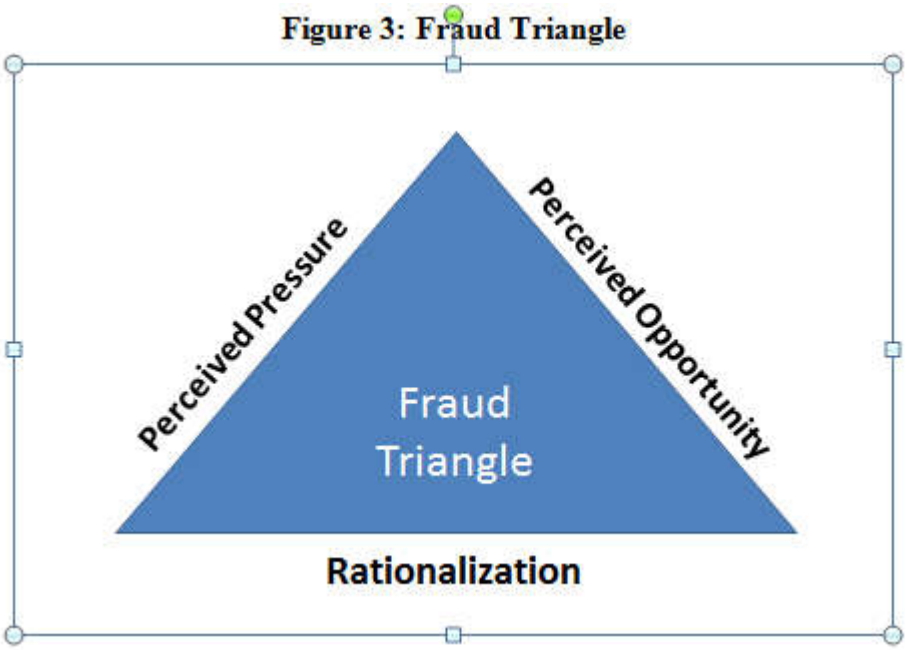
The **factors** that affect fraud are internal such as the design and effectiveness of internal controls, the organizational culture and the value system of employees, as well as external factors like the nature of business, the operating environment (industry sector, regulatory framework etc.).

It does not matter who is **accountable for FRM**. It could be the CCO, the CAE, a specialized Committee or anyone else. It is significant for an effective FRM to develop **synergies** and a spirit of **cooperation** among all participants, as well as to be independent and objective in their crisis and far from personal bias.

The fraud triangle theory

Another important part of fraud is the question, **"why does fraud occur"?** In 1950, Dr. Donald Cressey (Wells, 2013), a criminologist has developed the **"fraud triangle theory"** which explains what drive people to violate trust and commit fraud. Fraud triangle is the most accepted theory on how trusted people become trust violators. This theory introduces three interrelated factors which must be concurrent το commit fraud. These factors are summarized as pressure, opportunity and rationalization.

Figure 3: Fraud Triangle

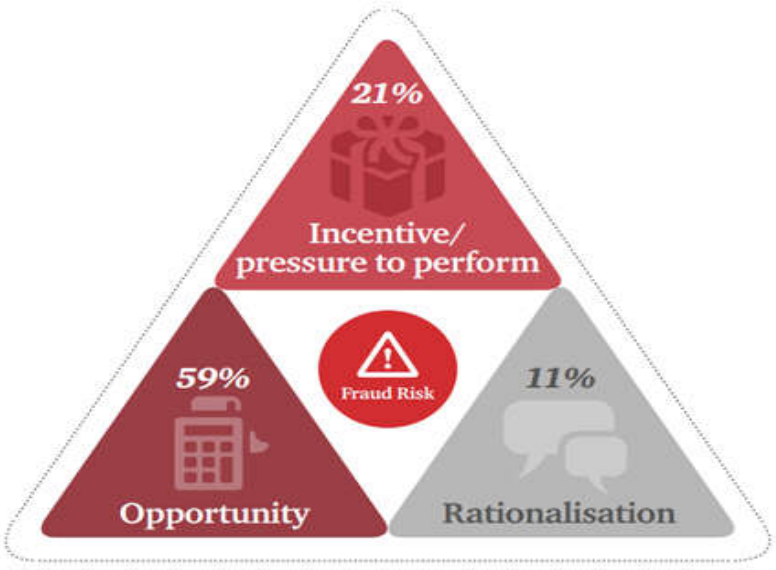


Source: https://wheatley.byu.edu/compromise-triangle/

It is worth mentioning 2018 Pwc survey "Pulling fraud out of the shadow" which encourages organizations to invest in people and exhibits through the fraud triangle theory, "what makes an employee commit fraud".

From what depicted in the following diagram, fraud starts with **incentives** for personal gain or due to a corporate pressure (21% contribution to the incident of fraud). It is prevented through openness. Fraud is followed by **opportunity,** which determined by the system of internal control (59% contribution to the incident of fraud) and finally by rationalization which is prevented by the organizational culture and ethical climate (11% contribution to the incident of fraud). These all three drivers should be present at the same time to commit fraud whereas they are addressed individually. The first could be influenced and managed in contrast with the 3rd (rationalization) that occurs within the human mind and it is harder to be influenced.

Figure 4: The fraud triangle: what makes an employee commit fraud?

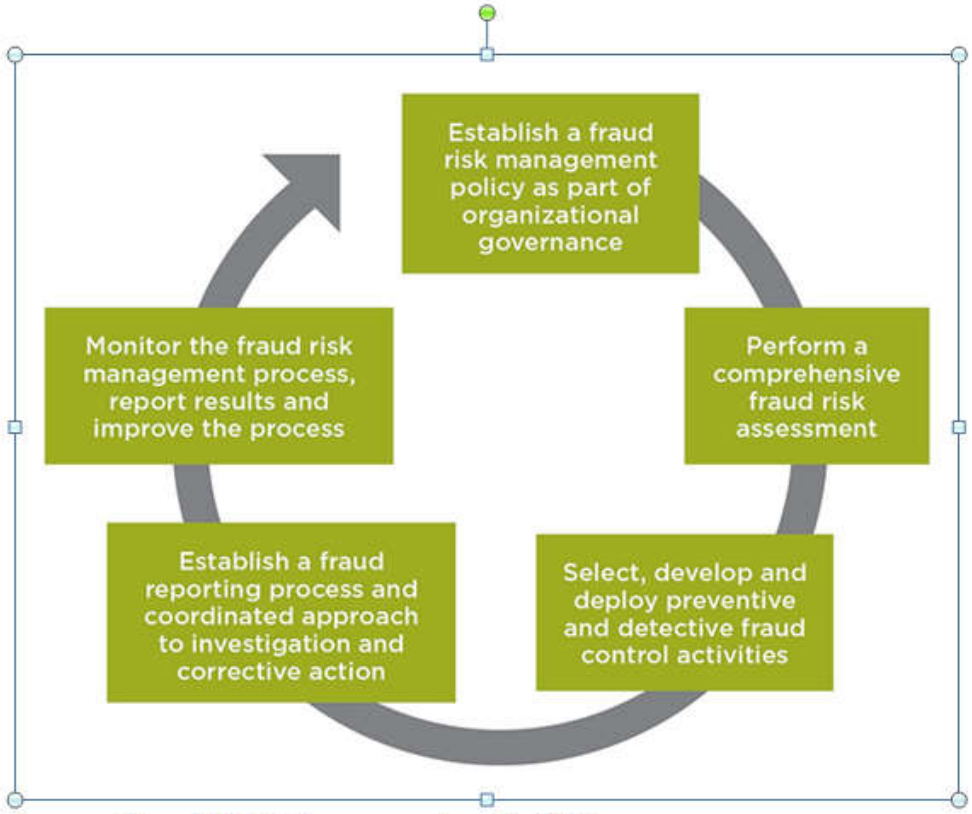


Source:https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

Fraud Risk Management

Fraud Risk management guide also recommends that organizations which use 2013 COSO Integrated framework should adopt separately a FRM program or process for assessing organization's fraud risks. This ongoing, comprehensive FRM process is depicted as follows:

Figure 5: ***Ongoing, Comprehensive Fraud Risk Management Process***



Source: Fraud Risk Management guide 2016

Corporate governance is not just rules and regulations, it is also "the tone at the top" a term used to describe the way the board and the management behave, giving an example to the rest of employees. This tone expresses the commitment of the management to specific behaviors and to the code of conduct (Protiviti, 2011).

The keystone of an effective anti-fraud program is the establishment of a strong value system that is reflected in the **code of conduct**. Code of conduct should take into consideration the minimum standards required by the law and the core values of the organization and advise employees to take the appropriate actions and decisions on everyday work. In case, they were not sure about the interpretation of any illegal

requirements they should ask the opinion of their supervisors or of the legal department (PCAOB AU Section 316 2002).

Fraud risk management guide states that **Board's and Senior Managers' role** is critical toward fraud risk. Therefore their attitudes reflect to the rest employees and send clear signals to the public and other stakeholders. They show to employees by words and actions that unethical behaviors cannot be tolerated.

It is worth mentioning that **corporate culture** is not "one size fits all" approach. It should be examined and aligned with organization's DNA or special characteristics so as to be effective. (Protiviti, 2011).

Within the framework of Fraud Risk Governance, it is required to be issued a **FRM policy** that demonstrates corporate culture coming from the BoD and the senior management and their commitment to integrity and ethical values in managing fraud risks (FRM guide 2016).

Essential components of a successful FRM should be the establishment of the **Audit Committee** or any other similar independent Committee, which should provide an oversight role, as well as fresh insights and guidance on FRM methodology. (KPMG, 2016).

Fraud Risk Assessment

COSO IC-IF and its **Principle 8** which stipulates that the organization should examine the potential for fraud when assess risks to the achievement of objectives is composed of four Points of focus as the following table:

Figure 6: COSO's I.C. – I.F. Principle 8 and its Point of focus

Principles		Points of Focus	
8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.	31	Considers various types of fraud
		32	Assesses incentives and pressures
		33	Assesses opportunities
		34	Assesses attidutes and rationalizations

Source: 2013 COSO Internal Control Integrated Framework

Key questions arising from COSO IC-IF 2013 are "why FRA has not been included in RA which is examined by the Principle 7*?",* "What is the qualitative differentiation between FRA and the traditional RA?", "Why did COSO want to distinguish fraud in a separate Principle?" and "What was its purpose?".

Firstly, FRA is a process conducted by the management, which identifies **fraud risks and schemes** within and outside the organization that need to be mitigated, whereas RA is the identification of **risks in general**, that could negatively affect the organization's ability to achieve its targets. FRA is a proactive tool that helps organizations to fight against fraud. FRA examines risk factors, taking into account the potential for fraud through the fraud schemes and Fraud triangle theory, whereas traditional R.A. focuses on risk factors in the assessing of risks.

FRA should include individuals from various divisions and with different knowledge, skills and competence. These individuals could be a combination of accountants, Human resources (HR) personnel, information technology (IT) personnel, internal auditors, legal & compliance personnel etc.

FRA could be conducted either as stand-alone examination or through RA (Managing the business risk of fraud –A practical guide). There are many substantial reasons why organization should conduct FRA separately from the traditional RA.

FRM guide also states that conducting a separate FRA provides greater assurance on fraud risks because it focuses on intentional acts and omissions which are connected with the achievement of company's targets and the strategy as well (2016).

Another distinguished difference concerns the element of **concealment** that contains the risk of fraud, as defined as an intentional, deliberate effort carried out by the management to cover up the truth. Consequently, every fraud risk includes a concealment strategy associated with false statement, false documents, false transactions, false representations etc. Thus, to conduct FRA is a prerequisite to understand and know the concealment strategy about these fraud schemes (**ACFE Presentation for FRA by Leonard W. Vona**).

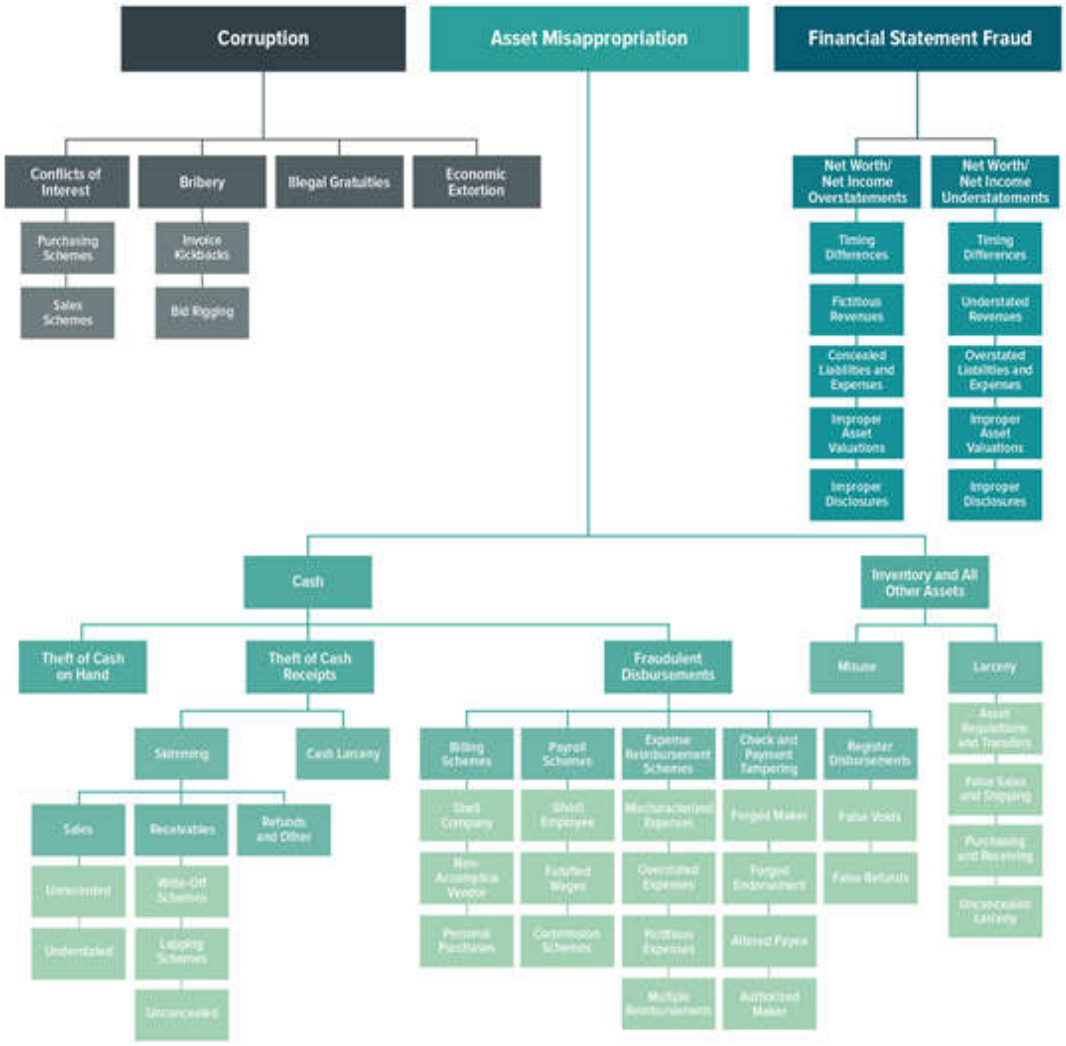
It is also very important to conduct FRA on a regular basis, in order to be always updated, and current. This happens when it is taken into consideration any changes in the internal environment, such as changes in processes, in personnel or in information systems and controls. The changes in the external environment (area, industry, market etc.) should be also taken into consideration such as economic crisis, cyber-attacks etc.

FRM guide suggests thinking cases where individuals might bypass controls and commit fraud, through Management override of controls or through collusion schemes. A basic anti-fraud control for those risks is the Segregation of duties. The report to the nations states that “the more people conspire the higher the loss occurs”. It also states “that half of the examined fraud cases include more than one perpetrator and results in much higher losses”. In those cases preventive controls cannot work effectively, so it is of a paramount importance to establish detective controls as to mitigate the risk by reducing the detection time (2016).

Classification of occupational fraud and abuse

There are three types of occupational Fraud and abuse, **Asset Misappropriation, Corruption and Fraudulent financial statements**. The ACFE has designed “The **“fraud tree”,** a chart where fraud schemes are classified per category.

Figure 7: Occupational Fraud and Abuse Classification System (The Fraud Tree)



***Source*:** http://www.acfe.com/report-to-the-nations/2018/

When Fraud occurs it produces cost and its size usually depends on the three main types of fraud. The Report to the nations for 2016 states that asset misappropriation is by far the most common type of fraud, occurring 83,5% of all cases, whereas corruption amounts to 35,4% and Financial statement Fraud to 9,6% respectively. On the contrary, Financial statement Fraud results to a median loss of 975 thousands $, Corruption to 200 thousands $ and Asset misappropriation to 125 thousand $ respectively, confirming the Pareto principle (The 2018 Report to the nations).

Leonard W. Vona, a financial investigator and anti-fraud expert, states that fraud is a cost of doing business and FRA is a key tool to do that by identified, understanding and building controls that are unique and specific to every organization. Unfortunately, no matter how hard organizations try, that cost cannot completely be eliminated as it always occurs. Thus, FRA is here to support organizations to manage and mitigate this particular cost. Therefore, conducting FRA is very important and substantial for every organization.

As, Wells, J. (2013) states, there are a lot of benefits conducting FRA:

- Help open communication and awareness about fraud.
- Guide organization on activities which highly exposed to the risk of fraud.
- Know the individuals that put the company at a greater fraud risk
- Reduce the exposure to fraud risk
- Helps to deal with fraud in cases that internal controls are failed, such as collusion.
- Supports organizations to set preventive and detective controls and thus deter fraud
- Comply with regulations and standards.

In addition Erick O. Bell and P. Jhang (2013) advise us that FRA can be failed due to the following reasons:

- Appropriate personnel are not involved in the process
- Assessment consists of an identification of risk factors only, and does not include an identification of schemes & scenarios
- Potential perpetrators are not identified
- Does not consider collusive fraud and management override of controls
- Lack of monitoring by the Audit Committee/Board
- Lack of follow up after identification of fraud risks and linkage to mitigating controls

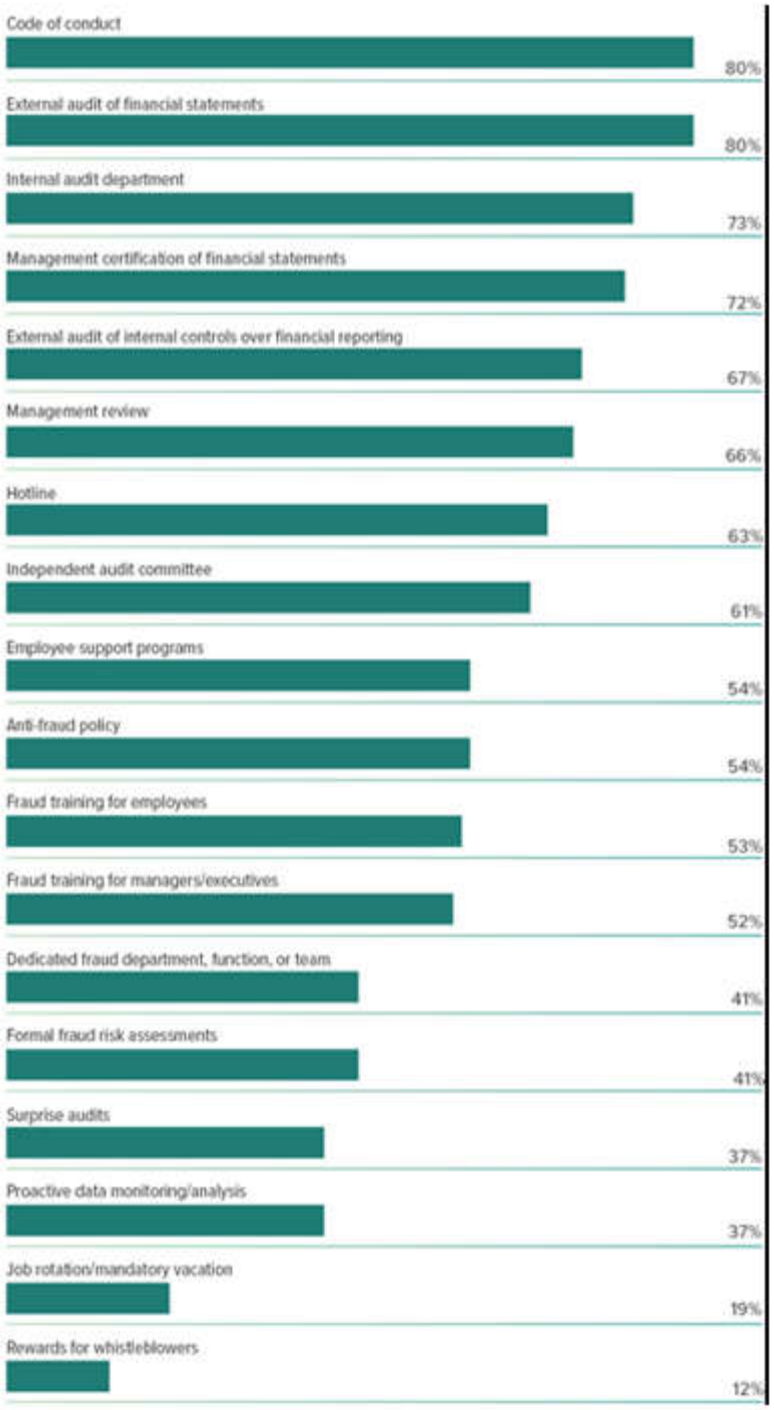
Anti-fraud controls

Fraud can happen to any organization. Size really does not matter. Small sized companies are more vulnerable to fraud because they have less resource to fight fraud than the large ones, so they use less anti-fraud controls. Small sized companies have to rely upon trust among the individuals and other third parties, which is not an internal control. Moreover the impact in small companies is higher than in large ones (Report to the Nations 2018).

Figure 8: Fraud in small businesses

Source: http://www.acfe.com/report-to-the-nations/2018/

Figure 9: What anti-fraud controls are most common?



***Source*:** http://www.acfe.com/report-to-the-nations/2018/

Although Organizations use anti-fraud controls, yet fraud is committed everywhere. The Report to the Nations 2018 presents a list of the most common anti-fraud controls at the victim organization the time the fraud occurred. Thus, the existence of anti-fraud controls does not provide absolute assurance against fraud.

Preventive anti-fraud controls are the first line of defense and therefore they are strong deterrent controls. Their Achilles' heel of preventive controls as **AICPA** mentioned is the management overrides.

It is obvious that preventive controls have many benefits although cost is included. Cost benefit analysis of preventive controls is not easy to be calculated whereas it has been approved by many surveys (Report to the Nations 2018), that they mitigate the risk and reduce the cost of fraud. CIMA 2008 states that the head of fraud investigation for a major bank made the following observation: "A £1m increase in expenditure on fraud prevention has led to a £25m increase in profits".

Fraud detection's key role is to identify fraud as quickly as possible so as to lose less money. Detection controls appear when preventive controls have failed. Fraud detection is an area where data analytics and other statistics could play an important role and help organizations to detect fraud soon (Bolton R. & Hand D. 2013).

Fraud awareness and training is considered very crucial in fighting against fraud and should be included in the corporate risk management strategy. It should be conducted periodically from the appropriate and well-trained staff, preferably by the Certified Fraud Examiner (CFE) to support management and employees. The ACFE is an international institute that puts continuously effort to educate and train CFE's in order to build competency and develop technical skills in dealing with fraud. CFE's may provide special knowledge and experience on the risk of fraud (especially for financial statement fraud) to the Audit Committee. They should cooperate with internal and independent auditors as to make coordinated efforts and have better results (PCAOB AU Section 316 2002).

It is very important for the company to establish an effective **hotline** in cases that somebody would like to address a complaint or to reveal unlawful facts. It is important to incorporate the whistleblower mechanism into corporate culture since it could be a major tool to detect fraud and deter wrongdoing (CIMA 2008).

Dyck.A. Morse.A. and Zingales.L. state that employees, media and industry regulations could blow the whistle on corporate fraud and not standard corporate governance players such as auditors, SEC and investors (2006).

Internal Auditors should have sufficient knowledge to identify fraud indicators ("red flags"), but they are not expected to have the expertise of CFE in dealing with fraud.

They should be in alertness for the occurrence of fraud when they execute their annual audit plan. Before that, they should have read FRA and evaluated it carefully, so as to be incorporated in their annual audit plan and asses anti-fraud controls. Internal Audit provides feedbacks to the Board and senior management about the design and effectiveness of anti-fraud controls and the overall FRA process. Internal auditors are one of the most important detective and deterrence control (PCAOB AU Section 316 2002).

Independent auditors have also a significant role in assessing and responding the risks of fraud to the Management and the Board (or the Audit Committee). They cooperate with internal auditors in making coordinated efforts when they evaluate the internal control system. They do have the alertness of the occurrence of fraud and they are both detective and deterrence control (PCAOB AU Section 316 2002).

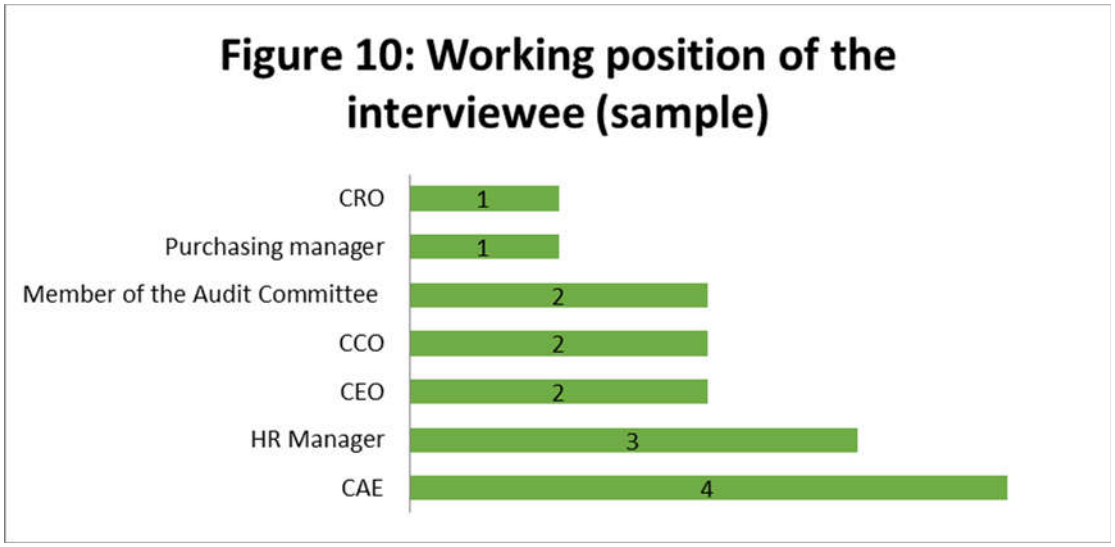
Managers in general are an anti-fraud control, but sometimes they override controls due to their authority (AICPA 2016).

CHAPTER 3: Empirical analysis

Introduction

The method of sampling chosen is judgmental, thus among the 15 organizations included are those with fraud awareness and those without fraud awareness.

For the purpose of this survey, 15 individuals have been selected and interviewed, which currently hold or used to hold key position in companies that operate in Greece (see figure 10). The sample includes organizations by various industry sectors (Figure 11), which employ from 100 to 9.000 employees (Figure 12). These individuals have expressed their opinion based on their working experience regarding FRM. In the following tables, demographic data such as interviewer's working position, turnovers, company sector, listed/not listed and ownership status, which are related with the sample, are demonstrated.



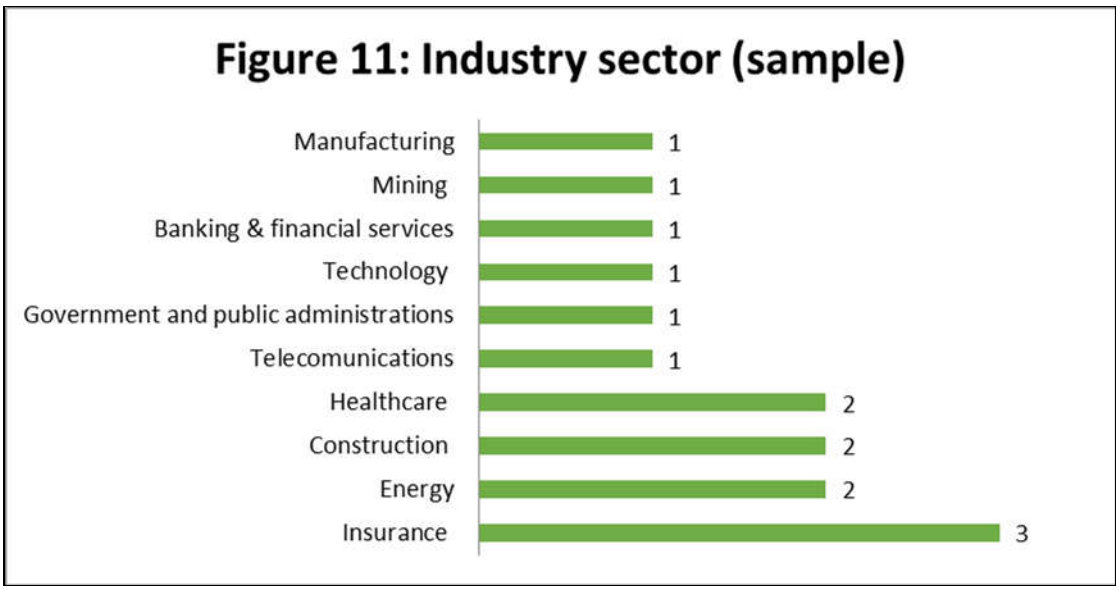


Figure 11: Industry sector (sample)
Manufacturing
1
Mining
1
Banking & financial services
1
Technology
1
Government and public administrations
1
Telecomunications
1
Healthcare
2
Construction
2
Energy
2
Insurance
3

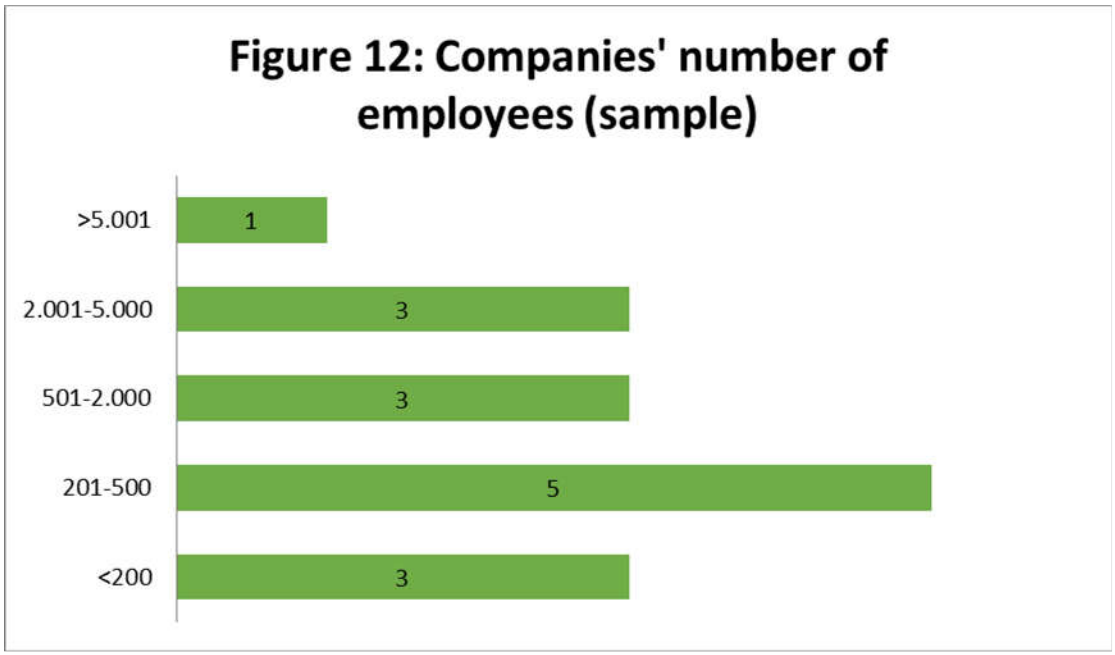
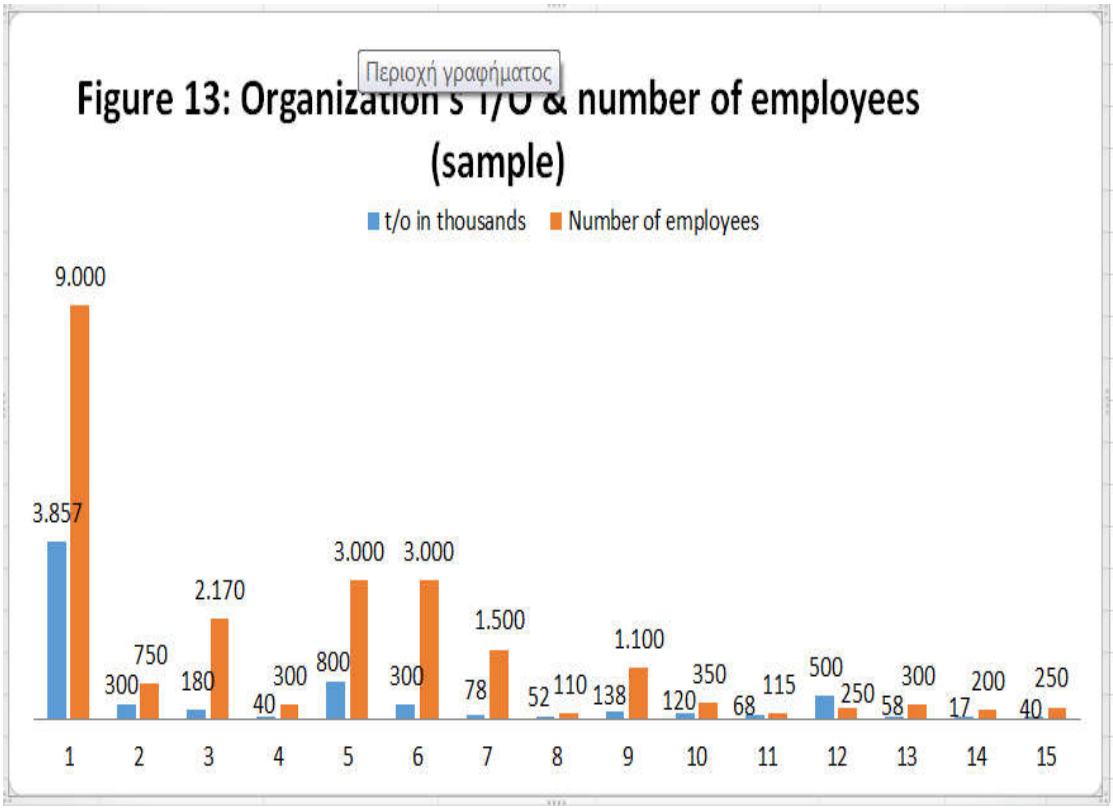


Figure 12: Companies' number of employees (sample)
>5.001
1
2.001-5.000
3
501-2.000
3
201-500
5
<200
3


Περιοχή γραφήματος
Figure 13: Organization's T/O & number of employees (sample)
t/o in thousands
Number of employees
9.000
3.857
750
300
2.170
180
300
40
800
3.000
300
3.000
1.500
78
110
52
1.100
138
350
120
115
68
500
250
300
58
200
17
250
40
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

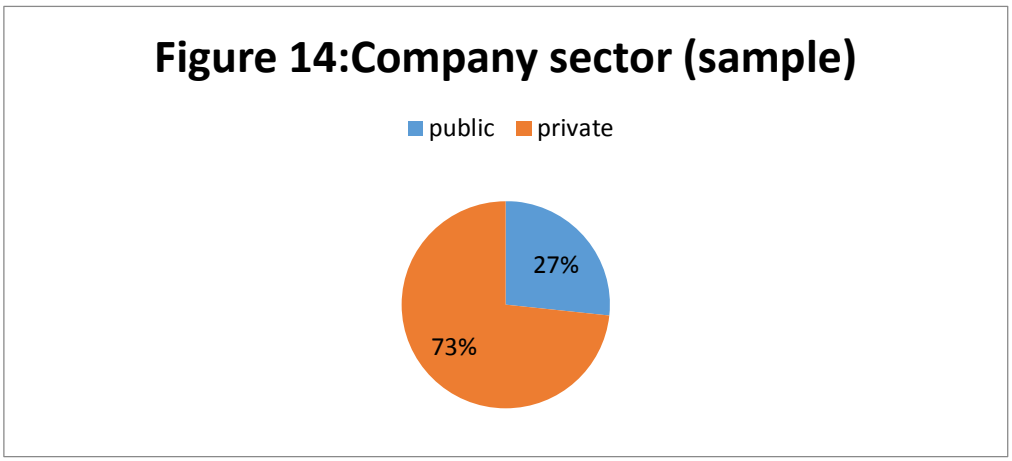
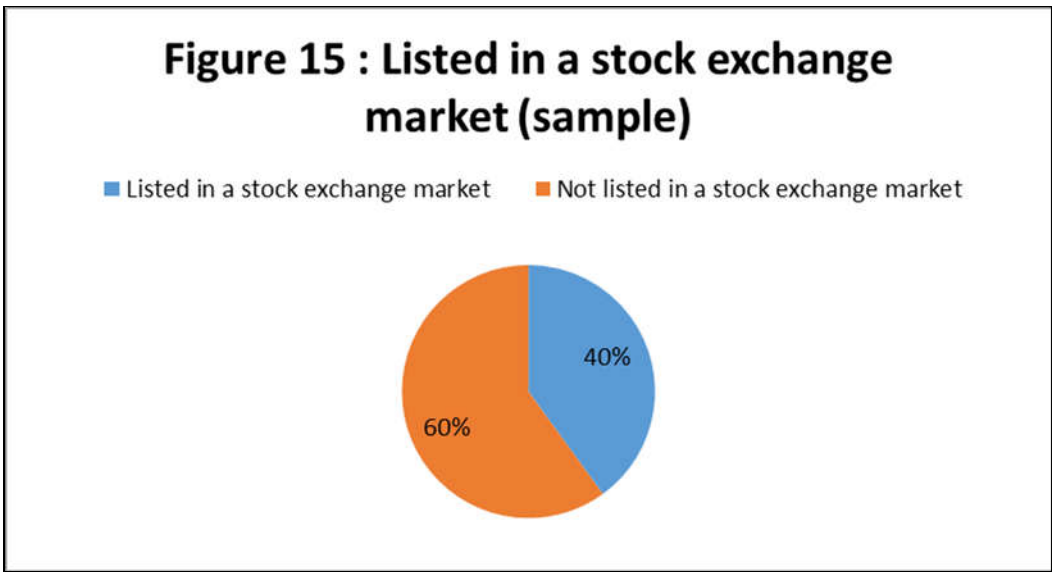
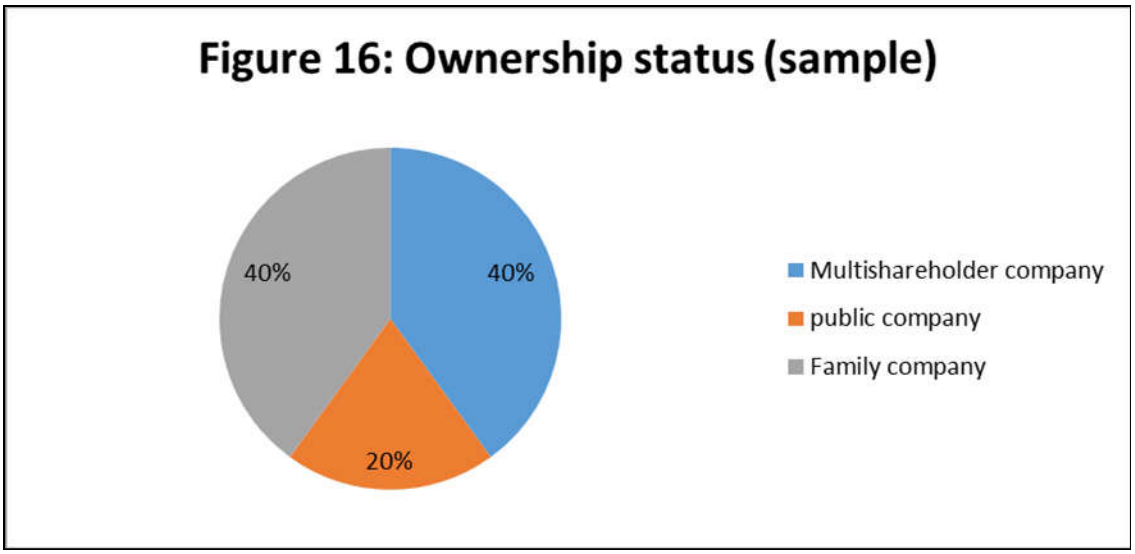
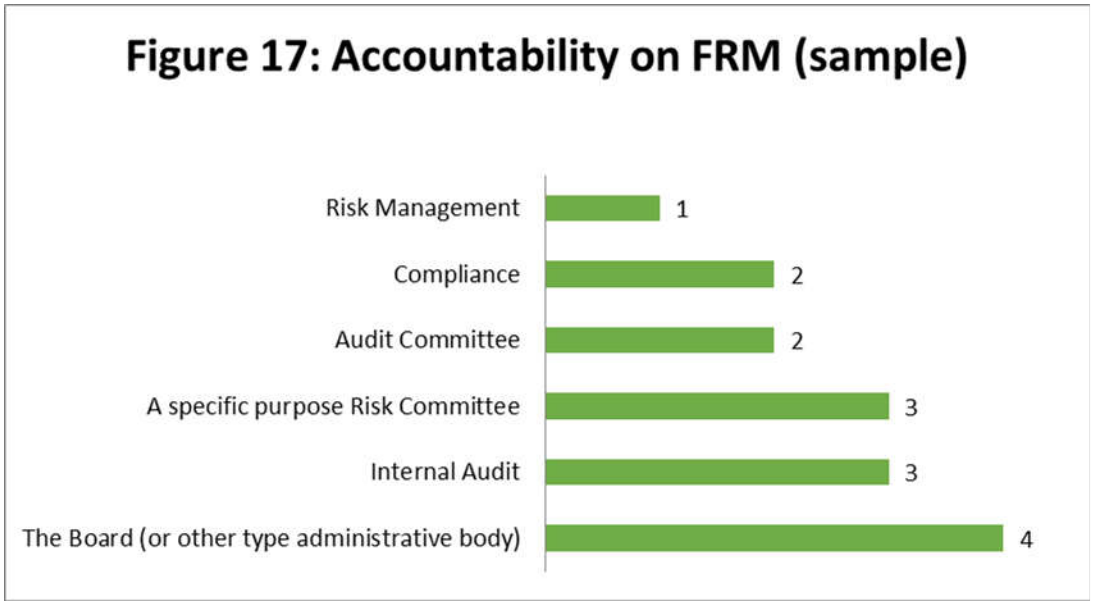


Figure 14:Company sector (sample)
public
private
27%
73%





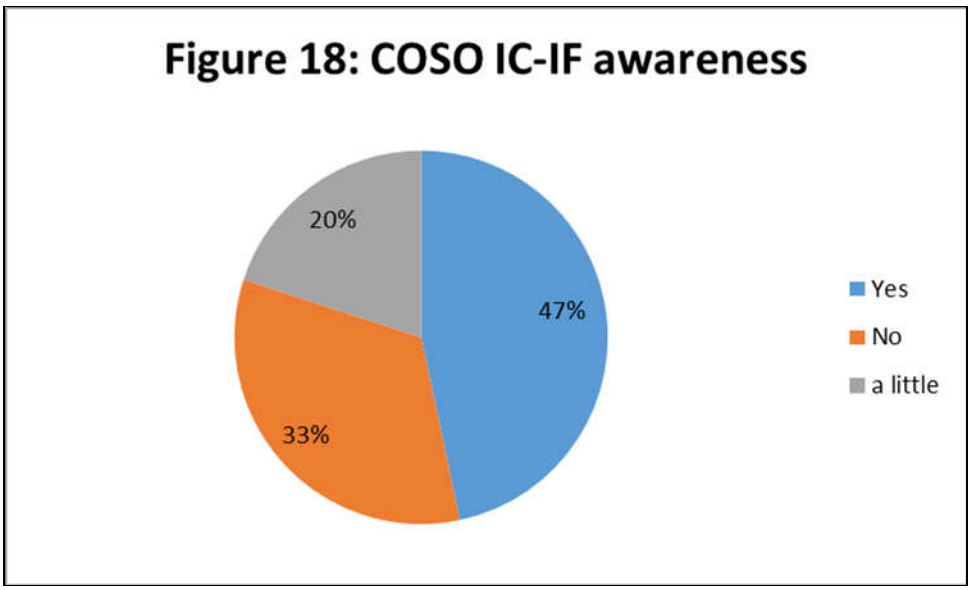
The accountability on FRM may have been assigned to various administrative bodies or working positions as it demonstrated below:

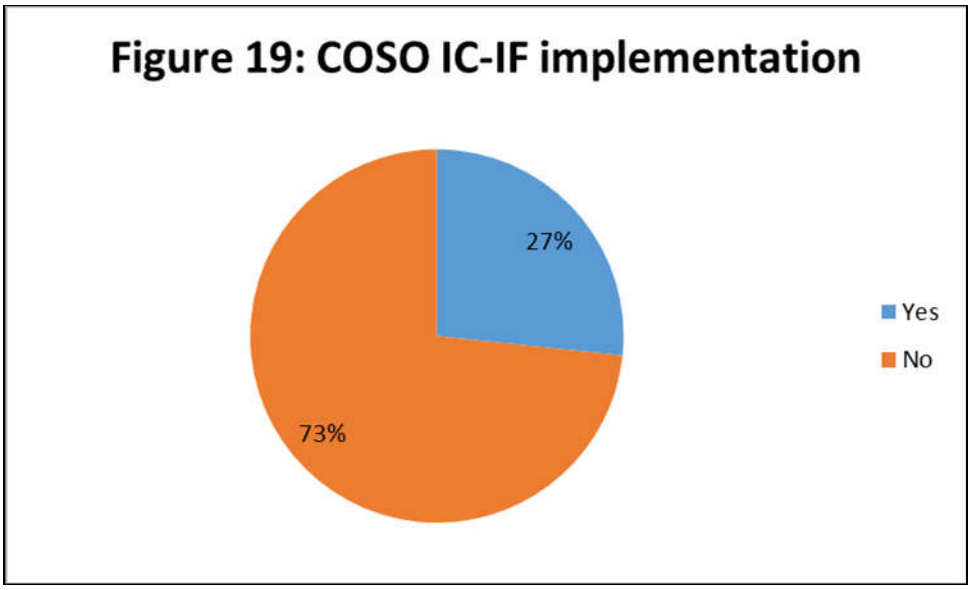


Organizations where the Board or any other administrative body has the accountability of fraud are those organizations that are not aware about COSO and its Principle 8, do not have an Audit Committee, do not prepare FRA and generally do not see any benefit at the moment to implement FRA. These 4 organizations as depicted in figure 17, consider the risk of fraud as low level risk.

COSO IC-IF

As demonstrated in Figure 18 & 19, 47% of the sample is familiar with COSO IC-IF, the 20% is a little familiar, whereas the 33% of them have not heard of it at all. On the other hand only 27% has currently implemented it. Additionally, none of the companies follows any other similar framework, apart from the listed companies in the Hellenic Stock exchange market - due to regulatory framework- followed by the Corporate Governance Code in the approach “comply or explain”.





There are 4 out of 15 organizations that implement COSO IC-IF. Three of them belong to Insurance and banking sectors and the last one to telecommunication sector. Two of them belong to a foreigner group of companies which require the adoption of COSO IC-IF and the rest of them due to specific requirements of the regulatory framework and law. It should be noted that none of the companies has adopted COSO IC-IF on a voluntary basis.

Regarding external auditors' sample, it is said that 5 of 7 are familiar with COSO IC-IF, while the remaining 2 are not respectively familiar. It should be noted that those two do not belong to the "big four" companies.

FRA

It is 1 out of 15 organizations (7%) that conduct FRA on a stand-alone basis, 11 out of 15 (73%) conduct FRA through the annual RA and the rest 3 (20%) do not conduct neither FRA nor RA as depicted in figure 20.

The organizations that conduct FRA on a stand-alone basis have already established a compliance department and show zero tolerance attitude against fraud and corruption.

The 11 organizations that include FRA in the typical RA, think that there is no need to conduct FRA on a stand-alone basis. It is worth mentioning that among these 11 organizations there are only 3 that use special techniques and knowledge to evaluate properly the risk of fraud in the preparation of FRA. The rest 8 out of 11 consider the risk of fraud as a basic risk factor, but it is a waste of time and effort to prepare it separately. These organizations do not involve appropriate personnel and they do not get an outsourcing support from experts to prepare FRA. Also, they do not examine fraud schemes and scenarios, collusion and management override of controls. A question arises on how fraud risk can be evaluated when they do not know or do not use specialized techniques and knowledge, like the fraud triangle theory, anti-fraud controls, related statistics etc.

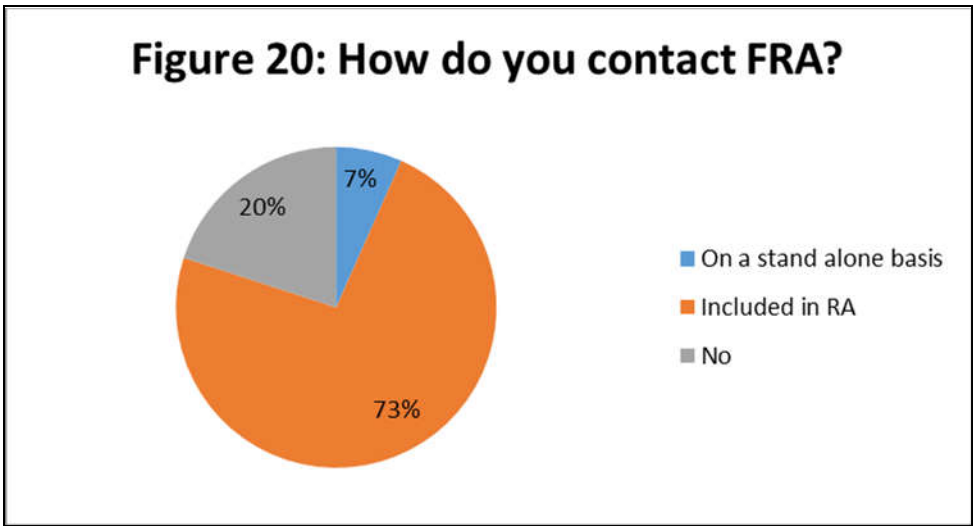
Finally, 3 out of 15 organizations, which do not conduct either FRA or RA, do not find any value in these processes. Two of them are small sized family companies and the last one belongs to the public sector.

An additional information regarding whether they use or would use an external service provider to support the implementation of FRA, is that 9 out of 12 organizations in order to prepare FRA they get a support from auditing firms or professional institutions (ACFE, IIA etc). The other 3 organizations that do not conduct FRA chose to get a support from an external service provider.

Finally, 11 out of 12 organizations that prepare FRA (either on a stand-alone basis or included in RA) conduct it annually whereas the other one on an ad hoc basis. Consequently 4 out of 15 organizations do not examine at all preventive measures to

manage the risk of fraud but they react occasionally and on an ad hoc basis (the same conclusion was in figure 17). These 4 organizations do not prepare Risk assessment because they consider that fraud will not happen to their organizations. Finally, regarding the rest organizations which include FRA in RA, 6 out of 11 do not make a good evaluation in the preparation of FRA. They do not use all necessary techniques and tools, they face fraud as an operating risk and when fraud appears then they start to invest in preventive and detective controls and other similar methods and systems. The risk of fraud is not always the same. It is changing from time to time. Risk has the potential to mutate depending on the time, on the space and on the circumstances, so it is not enough to be conducted once in 3-5 years, but at least annually and sometimes when occurs.

2 out of 15 examined organizations have not suffered from fraud. The 2 are family companies, without having established an Audit Committee and Internal audit function. They do not know anything about COSO-ICIF since they are small sized and juvenile. They have not faced any incident of fraud in contrast with the rest 13 companies which have either suffered greatly or had some small fraud incidents.



Corporate Governance

Audit Committees

In the sample, 6 out of 15 (40%) interviewees represent organizations Listed in the Stock Exchange Market, 8 out of 15 (53%) have established an Audit Committee and 11 out of 15 (73%) have established Internal Audit functions. All the above organizations that have established Audit Committees are enforced either by the stock exchange market regulations or by other regulatory frameworks and statutory provisions.

The Corporate Governance is considered to be a fundamental value of an organization and is tightly connected with the operation of the Audit Committees and Internal audit functions. In the sample 4 out of 8 (50%) cases, the Audit Committee operates more typically and less substantially. These members are not professionally competent, fully involved and also independent as appropriate. This fact originates from the law enforcement, since those companies have not realized the benefits that may result into an effective operation of such Committees.

From discussions with external auditors as well as with the main interviewees, the following conclusions came along about the causes of ineffective functioning of the Audit Committees:

- The number of meetings is the absolute minimum required by the law.
- The fees of the members of the Audit Committee are quite low regarding their efforts and their level of experience. It may be believed that their efforts are not as appropriate as it is required by the circumstances.
- The external auditors are mainly suggested and approved by the CFO's but are formally appointed by the Audit Committee or by the board, in cases where there is no Audit Committee.

For cooperation purposes, external auditors primarily discuss and negotiate with CFO's and not with the audit Committee, as required. This could be considered as a type of conflict, because it can affect the auditor's opinion about the fair presentation of financial statements increasing the risk of fraud.

What was noticed from the survey is that most of the times Audit Committees are involved passively in the selection of the Auditing firm.

Whereas some organizations operate typically, there are some which have taken advantage of the operation of Audit Committee in order to benefit the organization. Such companies mainly belong to a foreign group of companies and have a multi-shareholder structure. Those characteristics create the need of transparency and information existence for every shareholder as well as for the development of an effective internal control system throughout the organization.

An effective Audit Committee or alternatively a Risk Committee may oversight the Risk and the system of Internal Control and act as anti-fraud control, especially for large organizations where the risks emerge irregularly and require to be managed.

Moreover, Audit Committees or other similar Committees constitute the cornerstone (key factor) of RM and particularly the risk of fraud. Certainly, organizations without the existence of an Audit or Risk Committee could manage the risk of fraud but on the ad hoc situations, in a non-systematic matter where the duration and the size of fraud evolves out of control causing damage.

Professional certifications

As it is already mentioned above, fraud risk should be examined separately from the rest of the risks, otherwise it is difficult to assess and respond as required. FRA should be conducted by someone familiar and competent with fraud so as to identify and evaluate those risks. Sometimes it may be the internal auditor or the audit Committee, even better it could be assigned to a specialized department like risk and compliance.

40% of the examined companies had someone certified, a CIA, a CFE or a CISA, so as they are more disciplined and systematically effective and even better manage the risk of fraud. So, it appears that 4 out of 15 occupied more than one certified individual (a CIA, CFE or CISA). These are the only companies that are fully aware about COSO IC-IF and they are those that have implemented COSO IC-IF.

Additionally, there are 2 organizations that occupy only one certified (a CIA, CFE or CISA). They are not listed in a Stock exchange market, they have not established an audit Committee and they have prepared FRA without taking in account specialized techniques of fraud. In those cases certifications were not required by the organizations, but were derived from personal choices and initiatives of concerned individuals.

To employ someone certified in key positions is not only a single choice of an individual, but also a strategic choice of the organization in a more effective and efficient management of risks. The rest 9 of them do not employ any certified correspondingly.

The risk of fraud requires some special techniques that may be acquired by training, consulting or by being certified accordingly. As it mentioned above 6 out of 15 occupy at least someone certified, 8 out of 15 train its personnel occasionally and selectively and only 1out of 15 has not trained at all any employee respectively.

Anti-fraud controls

Table 1 presents a comparison between "The 2018 Report to the nations" and statistics occurring from the sample concerning anti-fraud controls. These data will be analyzed just below:

Table 1: Anti-fraud controls	2018 Report to the nations	Sample
External audit of financial statements	80%	100%
Internal audit department	73%	80%
Surprise audits	37%	73%
Code of conduct	80%	73%
Independent audit committee	61%	53%
Fraud training for managers/executives	52%	60%
Management review	66%	33%
Dedicated fraud department, function, or team (compliance)	41%	33%
Anti-fraud policy	54%	33%
Hotline	63%	27%
Fraud training for employees	53%	27%
Formal fraud risk assessments	41%	20%
Job rotation/mandatory vacation	19%	27%
Proactive data monitoring/analysis	37%	20%
Management certification of financial statements	72%	13%
External audit of internal controls over financial reporting	67%	7%
Employee support programs	54%	7%
Rewards for whistleblowers	12%	0%

Chartered accountants (External audit of financial statements) are those who sign and certify financial statements since they are imposed by the law. CAs are not selected because they charge less than the others but because they provide a reasonable assurance about whether financial statements are free of material misstatement. In the sample during the interviews was realized that in some cases CAs were used by the companies not as an anti-fraud control but as an imposed authority which is considered useful in verifying accounts and financial statements for its plausibility. In order to inform shareholders, institutions and any public concerned.

2 out of 6 CAs know few things about COSO IC-IF, whereas the other 4 are quite familiarized with the framework. So 1 out of 4 provides certification to one of the organizations of the sample, which is adopting all necessary financial controls based on COSO IC-IF.

5 out of 6 CAs consider that their audit scope is affected by the level of Corporate Governance of the examined organization, one from the initial RA and the last one from the size and the complexity of the organization and its financial statements.

5 out of 6 CAs stated that it is crucial to manage FR for both small and large sized companies. But it is not one size approach; it should fit the company's special characteristics and philosophy.

These CAs added that small sized companies usually face the risk of "Management overrides controls" due to the fact that these companies are mostly "one man show". Small sized company's controls do not usually exist or they are weak. There is no evaluation of the system of internal controls regularly and thus they are quite vulnerable to the risks of fraud and errors. Large sized companies have high reputational risk and exposure unlike the small ones. Small businesses are low cost businesses so they have fewer anti-fraud controls in place than large organizations, making them especially vulnerable to fraud.

In large sized organizations in contrast with the small ones, fraud detection is more difficult. It appears and lasts much longer. They also mentioned that fraud detection is not included in their scope; it is internal auditors' responsibility. 1 out of 6 CAs as opposed to the rest 5 asserts that small sized companies have low risks, whereas large ones have high risks.

The vast majority of the CAs of the sample agrees with the results of the 2018 Report to the nations regarding the system of internal control and preventive measures in small sized organizations.

In addition, CAs think that the duration of fraud detection lasts much longer in large sized companies than in small ones. The survey of the Report to the nations does not include directly the correlation between the duration of fraud with the size of business and the organization as well. But the Report to the nations has mentioned that both small and large sized companies are suffering mostly from Corruption which tends to last about 22 months. Small sized companies are also suffering from billing and from check and payment tampering schemes which tend to last about 24 months. The Report to the nation associates only the duration of fraud with the loss and also with the fraud schemes, but has failed to link them to the size of the organizations.

Based on the interviews and the results of the current survey it is deduced that the duration of fraud in small sized companies depend on the scheme. In small sized companies, assets misappropriation which usually has a medium likelihood and low impact can be detected quite fast. Corruption which affects lot small and large sized companies has a medium impact. As it was mentioned above lasts quite a lot, namely 22 months. Finally, financial statement fraud with a high impact and low likelihood lasts for about 24 months. Small sized companies have not developed any preventive and detective mechanism to prevent fraud. And when they do, they do not, detect it on time. Thus, in some cases (depends on fraud scheme) fraud may appear more often and last longer in small sized companies confirming the Report to the nation survey that states fraud causes almost double loss longer in small size companies than in large ones.

4 out of 6 CAs conduct internal control evaluation before they decide whether they can rely on internal control system of the examined organizations. They all consider that small sized companies usually have a weak internal control system.

They also declare that in order to establish a FRM philosophy primarily requires establishing corporate culture, show zero tolerance, provide accountability to internal audit or other related division and then record, evaluate and response to anti-fraud controls. They also mentioned that for a successful implementation a support by the Board is required. Moreover, it is crucial to employ a competent, mindful of personal biases facilitator and also to develop a collaborative effort with the involvement of all employees. They also mentioned that the most important criteria to prepare FRA and

consequently to establish FRM activity is the size and structure of the organization as well as the existence of multi-locations (subsidiaries, branches, warehouses).

There are 8 out of 15 (53%) organizations of the sample which have established both **Audit Committee** and **Internal Audit** function. These companies are all listed to various Stock exchange markets. Interviews and data gathering show that half of them have not adopted RM tools and techniques effectively e.g., they have not adopted COSO IC IF, they do not use FRA tools and techniques when they prepare FRA (one of them does not prepare it at all), they do not have neither a hot line nor a FRM manual etc.

4 of 15 organizations of the sample have not established an Audit Committee but they have established Internal Audit function. This fact jeopardizes the credibility and efficiency of the IA, due to the fact that they lack of full independence. In such cases Internal Audit which is considered as a strong anti-fraud control could lead to a weakening activity, a cost center activity and not a value added activity as primarily designed.

Although 73% of the examined organization conduct **surprise audits** (instead of 37% in the Report to the nations), they cannot be implemented in every process effectively. They conduct surprise audits to evaluate in real time internal controls, to count checks, inventory, fixed assets and securities mostly. Surprised audits though they are quite effective they are considered old fashioned and they are not one of the first line of anti-fraud controls.

Organizations should focus more in developing **proactive data monitoring**, which on the one hand are more costly due to the need to invest in advanced technological equipment but on the other hand provide continuous auditing and they are more time-effective and result-oriented in preventing and detecting deviations. The 2018 Report to the nations states that 37% of the examined organizations adopt “Proactive data monitoring” whereas in the sample of Greek companies only 20%, specifically only 3 organizations.

11 out of 15 organizations (73%) have issued a **Code of conduct**, whereas the rest 4 have not. It has been proven by the survey that the issuance of a Code of Conduct or a Code of Ethics has been adopted on a voluntary basis by almost all organizations. The 4 organization which have not issued a code of conduct at the time being are half of them public companies and the rest ones are developed small-sized companies. During the interview they have expressed their intention and their plans to issue a Code of

Conduct in the near future. Observing the sample, the majority of the organizations are concerned by the existence of a Code of Conduct and notice to renew it regularly so as to respond to the current situations. They consider Code of Conduct as a depository of the ethical values and also a basic anti-fraud control. Boards and senior executives are primarily involved in recording the basic points of this manual and try to transfer the content to all employees regardless of their working position. The examined organizations have included in the Code of conduct issues related mostly with HR, but also with Fraud and Corporate responsibility. It is worth mentioning that the volume of fraud is connected directly with organizational values which are expressed through the Code of Conduct.

However, it is noticed that some organizations are not interested in the compliance part but mainly in the existence of this manual. In the sample few organizations conduct internal audits of the Corporate Culture and thus on Code of conduct. Thus, Code of conduct should be evaluated and updated on a regular basis in order to ascertain its functionality.

Furthermore, the Code of conduct is a manual addressed not only to employees but also to every stakeholder. It is noticed in the sample that almost half of the organizations have issued or will issue Code of conduct which will be mainly addressed to employees and not to the third parties. In such cases, there is no possibility for third parties to reveal misconducts and unlawful practices.

In addition, it is very critical to associate Code of conduct with the “tone at the top”, which as it was mentioned above as it describes the ethical climate of the organization leading by Board members and senior executives. In most interviews was reported that Board members were involved in everyday business which defines what is tolerable or not, regarding the ethical behavior when employees carry out their duties. They told that Board members and senior executives manage by example. In this way, employees uphold behaviors and actions of Board members and upper management and follow them; in a nutshell they do what their bosses do. Apart of these organizations, in the sample there are also group of companies where business units are located at different points and the day to day operations could not be controlled and managed as appropriately. Then “tone at the top” should be expressed through the Code of Conduct which must be checked by auditors and other related personnel regularly. In these cases, as well as in other similar cases there should be additional

measures such as training, hot line mechanisms, fraud awareness and other activity which can help corporate culture in the entire organization.

When organizations are blind to small scaled frauds and when they sometimes encourages employees to commit fraud for the benefit of the organization and in the expense of society, then in the near future they will face it as a serious problem. In other words, these organizations will facilitate the rationalization part for the employee who would be able to commit fraud.

Hence, corporate values should be tightly connected with the human factor. It plays a paramount role in an organization in order to establish an ethical environment where transparency, trust, security and integrity will prevail.

A code of conduct or any anti-fraud policy is not enough to fight fraud, unless it is associated with appropriate corporate practices and culture. Many times policies describe what should be done and corporate culture what really happens. This gap must be a matter of concern so as to take actions.

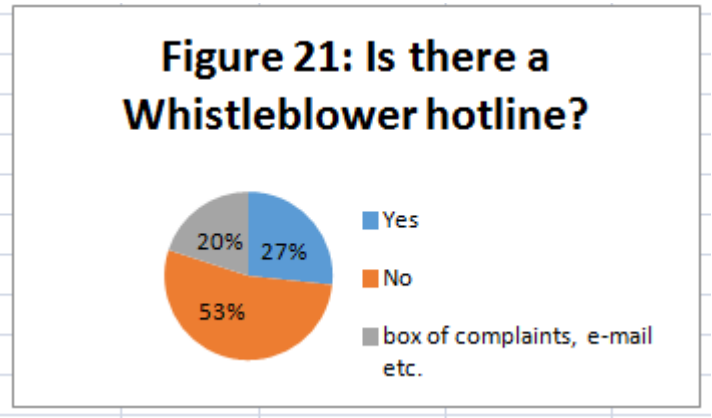
Whistle blowing mechanism is a new trend in fraud detection and acts primarily as an anti-fraud control. It is a reporting hotline that protects the organization and the society as well. Although, it has not been accepted by several societies and countries, because it must be consistent with their legal framework and culture. Due to the fact that the concept is quiet new, it has not thoroughly been clarified by the legal part. Thus, it needs time to be accepted by the entire society.

In figure 21 few organizations of the sample 4 out of 15 (27%) have already adopted a whistleblower hotline. They use it as a fundamental tool to detect fraud and various misconducts. They connected it with the Code of conduct so as to detect any violations not only directly connected with fraud but also with employees who can affect the ethical climate and therefore fraud.

Moreover, 8 out of 15 (53%) cases concern organizations which have not already established any mean of complaints and grievances. They consider that this mechanism does not fit with the European culture and especially with their company's culture. They do not accept it as an effective anti-fraud measurement, but they think that it will possibly disturb employees' relations. They consider it as a "squealer".

Lastly, 3 out of 15 have other means of complaints like box of complaints and e-mail. These organizations are well-considered to adopt a Whistleblower hotline but they

hesitate frightened by uncomfortable reactions from the employees and instead of getting benefits they engender an unpleasant atmosphere.



Whistleblower hotline success is attributed to the statutory acts and relative efforts by the appropriate bodies and above all support from the legal framework and relevant authorities.

From CAs and interviewees opinion it was said that in a whistleblower hotline is required to be involved someone from the Board and not any other operational manager which are not independent or any third party as it is customary to be in U.S.A. organizations. They formulate that Whistleblower hotline cannot provide full confidence to the whistleblowers. In cases that the hotline receiver is not independent or a trusty person, whistleblowers are afraid of retaliations and unpredicted consequences in their working environment.

There are some strong anti-fraud controls in the Report to the nations which were not developed by the organizations of the sample. These are:

72% of the organizations of the Report to the nations use as anti-fraud control **"Management certification of financial statements",** whereas only 2 out of 15 in the sample respectively. These 2 organizations of the sample have adopted it due to the regulatory purposes (one organization belongs to a foreigner Stock exchange market and for the other one it has been enforced by the government). Organizations from the Report to the nations have developed this useful anti-fraud control because many stock exchange markets worldwide, especially the most developed require from the management of the listed companies to certify for the accuracy of financial statements

(SOX Section 32). Thus, the aforementioned measure needs to be expanded to more markets, because it will not be adopted by any organization on a voluntary basis.

The same conclusions are also coming from anti-fraud control **"External audit of internal controls over financial reporting"**. 67% of the organizations of the Report to the nations use it as anti-fraud control (SOX Section 404), whereas only 1 organization of the sample and this is due to the government enforcement.

Another important anti-fraud control of the Report to the nations is **"Employee support programs"**. It has been developed by 54% of the organizations, whereas only 1 in the examined sample. This is due to new practices and trends which are not well-known to the Greek working environment.

Detection methods

Table 2 presents a comparison between "The Report to the nations" and statistics occurring from the sample concerning detection methods.

Table 2: Detection method	2018 Report to the nations	Sample
Internal audit	15%	33%
Tip	40%	27%
External audit	4%	20%
Management review	13%	7%
Notified by law enforcement	2%	7%
Document examination	4%	7%
By accident	7%	0%
Other	6%	0%
Account reconciliation	5%	0%
Surveillance/ monitoring	3%	0%
IT controls	1%	0%
Confession	1%	0%
	100%	**100%**

It seems that **tip** is the most effective anti-fraud control in the Report to the nations whereas in the sample it is second in priority. As it was mentioned above 4 out of 15 organizations have already established a whistleblower hotline, 3 out of 15 have alternative means of complaints like box of complaints and e-mail and the rest 8 have not established any means of complaints. These 8 organizations consider that they

could develop channels of communication with employees, so as to receive information about misconducts. This fact is mainly noticed in small-sized organizations where due to the size and the complication of operations, there is no necessity to establish a line of complaints. They cannot take any advantages from these mechanisms which were described as critical anti-fraud controls. It is worth mentioning that hotlines are not only a detective control but also a preventive one, since they deter fraudsters from committing a fraud.

In the sample, **internal audit**'s role is appreciated by the organizations as a major anti-fraud control and as the basic mean of detection, whereas in the Report to the nation has less importance. It could be strongly justified from the fact that in the Report to the nations thousands of cases are included, whereas in the sample only 15. Another explanation concerns the fact that in the sample organizations have not developed various detective methods and they are based mostly in Internal audit, tips and External audit. Especially organizations without any FRM approach are totally based on External auditors in detecting possible fraud cases. The less organizations are concerned about fraud, the less they implement preventive measures and they are waiting to manage fraud when it appears.

This study provides evidence on how organizations manage the risk of fraud. Various methods are being followed and those that are more aware of fraud are organizations listed in Stock exchange market. From the sample studied above, only 4 organizations have developed all best practices concerning fraud awareness, the establishment of an Audit Committee; of an independent internal audit or a Compliance department, as well as Risk Management. These 4 organizations implement COSO ICIF and 2 of them obtain certification of implementing COSO IC-IF regarding Management certification of financial statements and also of internal controls over financial reporting by external auditors. The accountability of fraud belongs to either to IA, RM or Compliance dpt. These organizations train their employees at all levels regarding fraud and evaluate regularly critical antifraud controls and conduct fraud-risk gap analysis. It should be noted that 3 out of 4 are listed companies and the remaining one is governmental. As a consequence, regulations and law enforce organizations to adopt anti-fraud controls, which if not imposed would not be adopted.

It should be acknowledged that fraud could occur in any entity, at any time and could be perpetrated by anyone. It does not matter who will be accountable for fraud but to

be assigned to someone. He could be the CAE, the CCO or anyone else who could coordinate it effectively.

The Report to the Nations on occupation fraud and abuse in their survey of 2018 states that the typical organization loses 5% of revenues in a given year as a result of fraud. This is also confirmed through the research; 13 out of 15 have suffered from fraud incidents.

CHAPTER 4: Conclusions

The current methodology and the primary data selected by the researcher came to the following conclusions:

- Fraud is associated with **organization's structure**. Small sized organizations face FRM as cost center activity. Moreover, family owned enterprises consider that they can control everything inside their corporation. When they start to grow up and expand through branches and subsidiaries they will find out that corporate governance should be reexamined and speed up to restrain any damage while consuming resources more than it was required in normal circumstances. Proactive measures cost less than damage control.
- Fraud concerns Greek entities which have developed **weak Corporate Governance** and consequently Fraud Governance (Principle 1 of FRM guide). In Greece there is a legal framework but it is required regulators to be more involved. It is considered through the emerging crisis to readjust the legal framework in order to identify relevant risks. The problem is not the legal framework but its enforcement. As a consequence, institutions are becoming more interested in Corporate Governance and FRM.

- Most of the organizations **are not familiarized and thus cannot understand FRM**. They consider fraud as something alien which does not affect them and consequently does not concern them. If they become acquainted with FRM they will acknowledge that it works for their benefit. FRM is not a cost center activity; instead it is a value added activity. It is conducted so as to get benefits like monitoring possible fraud schemes, cultivating a corporate culture and saving money. Understanding how to properly identify and assess potential fraud risk will help an organization to develop and implement an effective anti-fraud program which can reduce the potential organization's risks associated with fraud.

The results of the research could be useful to organizations which **need to adopt anti-fraud measures** as well as to those organizations **with a high rate of inherent fraud risk**. It is also useful to institutions which are interested **in getting insights about FRM**. This study could stand as **a guide** in order to understand and implement FRM successfully.

Since the data of the research were gathered through open interview questions and not through a written questionnaire, some answers cannot be justified precisely. The sample includes only Greek companies due to the fact that there were no contacts with foreign group of companies. Moreover, critical and sensitive information about fraud incidents could not be revealed due to confidentiality reasons.

From the aforementioned conclusions it is recommended:

- To conduct **a special research** by Professional bodies like ACFE Greece. Such a research could include data and opinions from a bigger sample of domestic companies, thus the results could easily be generalized.
- To be used an **e-platform** that will ensure the anonymity of the participants.
- **Regulators should be more involved** in order to enhance and monitor Corporate Governance and
- Actions regarding **fraud awareness** to be conducted by institutions and other relevant organizations and local entities

The key to mitigate the risk of fraud is to be vigilant, mindful and prudent and along with it to establish anti-fraud mechanisms to prevent and detect fraud. It is easy to get a list of antifraud controls from benchmarking and implement them. But do they fit to every organization? Do these controls work effectively to both small and large sized companies, to every industry sector, to different mindsets, types of management as well as national and religious groups? These questions can be answered by adopting FRM which is appropriate with each company's specific characteristics.
What should be known is that there is no immunity to fraud in any organization.

Annex 1

Questionnaire addressed to organizations

DEMOGRAPHIC DATA

Industry sector:	
Listed in a Stock exchange market:	
Interviewee' s department:	
Annual turnover:	
Company' s number of employees:	**< 200**
	201– 500
	501 – 2.000
	2.001 – 5.000
	> 5.001

Control environment

1. Do you think fraud is a problem for business in general? How Risk of Fraud is related to the operations and the strategy of the organization?
2. Is there a chart of organization? Have you issued policies and procedure for operating functions? Have you assigned roles and responsibilities as well as accountability for operating functions?
3. Do you have an effective Audit Committee or other similar Committees? Which is the Board's role regarding F.R.M.?
4. In what respect and extent has been determined by the organization, its tolerance regarding different types of fraud? Does your organization expect and demonstrate "zero tolerance "attitude" in fraud?
5. Have you ever encountered fraud cases in your organization?

Yes,

No,

N/A

If "Yes", what has the organization done for it (regarding the system of internal control)?

6. Are you aware about COSO I.C.-I.F. and especially about its Principle 8? Have you adopted it or you use an alternative framework?

   Yes,

   No,

   N/A

7. Do you train employees through various means periodically? Do you examine the professional competency and sufficient knowledge especially those who hold key positions?

Risk Assessment

8. Do you conduct RA? Does fraud included in RA or you conduct it on a stand-alone basis? Explain the reasons why.

   a. Included in RA

   b. On a stand-alone basis

   c. Not consider Fraud Risks

9. What are the reasons of not conducting FRA?

   a. FRA does not fit to my organization (size, culture etc.).

   b. It is a cost center. We consider that implementation cost is higher than its benefit.

   c. We examine it when there is a potential risk.

   d. We intend to implement it, somewhere in the near future.

e. Other reason

10. Which are the reasons of conducting FRA?

    a. Commitment to Professional standards.

    b. It is a Compliance issue.

    c. The Cost of Fraud is high.

    d. Fraud is a business Risk that has to be managed.

    e. Other reasons……...

11. How often do you conduct FRA?

    a. Every 3-years

    b. Annually,

    c. Semi-annually

    d. Quarterly

12. Who is the coordinator?

    a. C.E.O. or G.M.

    b. Internal Audit

    c. C.F.O.

    d. C.C.O.

    e. C.I.O.

    f. Legal Department

    g. HR

    h. Other

13. If you don't conduct fraud risk assessment, how will you implement it, through internal or external service provider? Would you need any third party support?

14. When you prepare FRA do you take into account fraud schemes and scenarios? Do you examine them and how?

a. Fraudulent financial and non-financial reporting,

b. Misappropriation of assets and

c. Corruption

15. Do you consider Management override process level controls through their level of authority when preparing FRA?

    Yes

    No

16. Do you use "Fraud Triangle theory" or other kind of tools when preparing FRA? In the assessment of fraud risks do you examine Motives (incentives and pressures), any opportunities to commit fraud and cases where senior management and other authorized personnel might justify or conceal any improper acts?

17. Why FRA is a value added activity?

    a. Identify and Understand Fraud Risks and potential schemes.

    b. Evaluate anti-fraud controls.

    c. Enhance corporate awareness on the risk of fraud.

    d. Support organization in achieving their targets.

    e. Other

Control activities

18. Are there any critical processes? What kind of controls do you have established for them? Are these controls preventive and/or detective? Do you segregate the duties on critical processes?

19. Which are the most effective anti-fraud controls in your organization? Do they help in fighting with fraud?

    a. Whistle and blower hotline

    b. Fraud awareness

c. External auditors

d. Internal auditors

e. Code of conduct

f. Conflicts of interests

20. How do you communicate all Policies related to fraud?

Information & Communication

21. Are there any reporting hotlines throughout the organization?

22. Is there any system of anonymous accusation (whistleblower hotline)?

23. Is there any policy for coordinated approach to investigative and corrective actions?

Monitoring

24. Do you conduct evaluations (regular, periodic or ongoing) for the above 4 principles, that they both exist and operate effectively?

25. Is there a regular program to monitor the deviations of the above 4 principles, so that corrective measures can be taken? Is there any participation of the senior management?

Annex 2

Questionnaire addressed to chartered accountants.

1. Is your organization concerned about Fraud and how? Do you think fraud is a problem for business in general?
2. Have you ever detected fraud in the auditee organizations?

   Yes,

   No,

   N/A
3. Does it matter the size of the fraud in auditing?

   Yes,

   No,

   N/A
4. How difficult is to manage information gaps and other deficiencies with the Board and CFO?
5. Are you aware about COSO I.C.-I.F. and especially about its Principle 8?

   Yes,

   No,

   N/A
6. Does your organization conduct RA or FRA when preparing the audit plan (budgeted hours, processes)?

   Yes,

   No,

   N/A
7. Do you examine company's risk assessment and audit report so as to rely or not on them?

Yes,

No,

N/A

8. Who is mostly cooperating with you regarding FRA ?
9. What do you examine in FRA?

a. Do any of your employees (auditors) have been certified as CFE? What other certifications they have?

b. When you prepare FRA do you take into account fraud schemes and scenarios? Do you examine and how?

i. Fraudulent financial and non-financial reporting,

ii. Misappropriation of assets and

iii. Corruption

c. Do you consider Management override process level controls through their level of authority when preparing FRA?

Yes

No

d. Do you use "Fraud Triangle theory" or other kind tool when preparing FRA? In the assessment of fraud risk do you examine Motives (incentives and pressures), any opportunities to commit fraud and cases where senior management and other authorized personnel might justify or conceal any improper acts?

10. Why FRA is a value added activity?

a. Identify and Understand Fraud Risks and potential schemes.
b. Evaluate anti-fraud controls.
c. Enhance corporate awareness on the risk of fraud.
d. Support organization in achieving their targets.

List of abbreviations

AAA – American Accounting Association

ACFE – Association of Certified Fraud Examiners

AICPA – American Institute of Certified Public Accountants

BoD – Board of Directors

CA – Chartered accountant

CAE – Chief Audit Executive

CCO – Chief Compliance Officer

CFE – Certified Fraud Examiner

CFO – Chief Financial Officer

CIA – Certified Internal Auditor

CIMA – Chartered Institute of Management Accountants

CISO – Chief Information Security Officer

COSO – Committee of Sponsoring Organizations of the Treadway Commission

CRO – Chief Risk Officer

Dpt – Department

ERM – Enterprise Risk Management

FEI – Financial Executives International

FRA – Fraud Risk Assessment

FRM – Fraud Risk Management

HR – Human Resources

IA – Internal Audit

IC – IF – Internal Control –Integrated framework

IIA – Institute of Internal Auditors

IMA – Institute of Management Accountants

IPPF – International Professional Practices Framework

PCAOB – Public company accounting oversight board

RA – Risk Assessment

SEC – Securities and Exchange Commission

SOX – Sarbanes-Oxley Act of 2002

References

1. Bell,E. & Jhang,P. (2013), *Developing a Fraud Risk Management Program.* Available at: https://chapters.theiia.org/san-diego/About/Documents/Fraud%20risk%20management%20program.pdf
2. Bolton R. & Hand D., (2013). Available at: https://projecteuclid.org/euclid.ss/1042727940
3. Chartered Institute of Management Accountants (2008), *Fraud risk management: A guide to good practice.* Available at: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf
4. Committee of Sponsoring Organizations of the Treadway Commission, (2016), *COSO Fraud Risk Management Guide*. Available at: https://www.coso.org/Pages/PageNotFoundError.aspx?requestUrl=https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive
5. Committee of Sponsoring Organizations of the Treadway Commission, (1992), *COSO Internal Control Integrated Framework.* Available at: https://www.coso.org
6. Committee of Sponsoring Organizations of the Treadway Commission, (2013)*, COSO Internal Control Integrated Framework.* Available at: https://www.coso.org
7. Committee of Sponsoring Organizations of the Treadway Commission, (2004)*, COSO Enterprise Risk Management — Integrated Framework.* Available at: https://www.coso.org
8. Committee of Sponsoring Organizations of the Treadway Commission, (2017)*, COSO Enterprise Risk Management — Integrated Framework.* Available at: https://www.coso.org
9. Dyck.A. Morse.A. & Zingales.L, (2006), Who blows the whistle on corporate fraud. Available at: http://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1476509
10. Ernst & Young (2014), *Updated 2013 COSO Framework — Fraud risk assessments.* Available at: http://www.ey.com/Publication/vwLUAssets/ey-coso-framework-fraud-risk-assessment/$FILE/ey-coso-framework-fraud-risk-assessment.pdf

11. KPMG (2016), Audit Committee Forum - Guidelines for the Audit Committee's assessment and response to the Risk of Fraud. Available at: https://home.kpmg.com/content/dam/kpmg/mu/pdf/mu-acf-position-paper-4.pdf
12. Protiviti- Independent Risk Consulting (2011), *Evaluating your Anti-Fraud program.* Available at:i-https://www.protiviti.com/US-en/insights/suggestions-evaluating-your-anti-fraud-program
13. Public company accounting oversight board (2002), Consideration *of Fraud in a Financial Statement Audit.* Available at: https://pcaobus.org/Standards/Archived/Pages/AU316a.aspx
14. Pwc (2018), *Global Economic Crime and Fraud Survey - Pulling fraud out of the shadows*. Available at: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf
15. The American Institute of Certified Public Accountants (2016), Management override of internal control: The Achilles' Heel of Fraud Prevention. Available at: https://www.aicpa.org/ForThePublic/AuditCommitteeEffectiveness/DownloadableDocuments/achilles_heel.pdf
16. The Association of Certified fraud examiners (2018), *Report to the Nations on Occupational fraud and Abuse*. Available at: http://www.acfe.com/report-to-the-nations/2018/
17. The Institute of Internal Auditors & Association of Certified Fraud Examiners & the American Institute of Certified Public Accountants (2008), *Managing the business risks of fraud: A practical guide.* Available at: https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf
18. The Sarbanes-Oxley Act (2002), Available at: http://www.soxlaw.com/
19. Video. The Association of Certified fraud examiners, *Presentation for fraud risk assessment by Vona,L*. Available at: http://www.acfe.com/course_samples/FraudRiskAssessment/presentation_html5.html
20. Wells,J. (2013), *Principles of fraud Examination*, Wiley 4th edition.