Università
Ca'Foscari
Venezia

Master's Degree

in Management

Accounting and Finance

Final Thesis

The WorldCom fraud under the COSO framework analysis

Supervisor
Ch. Prof. Simone Mazzonetto

Assistant supervisor
Ch. Prof. Caterina Cruciani

Graduand
Rossella D'Antonio
Matriculation number
852548

Academic Year 2020 / 2021

To my special family, for all their love and support.

ABSTRACT

Through data processing, the Association of Certified Fraud Examiners has estimated that organizations suffer losses of 5% of their revenues to fraud each year. Considering the huge impact this has on our economy, the first part of the paperwork will be focused on the origin of Fraud and on the different categories in which it is subdivided, dwelling in particular on the well-known *Fraud triangle theory* introduced by Donald R. Cressy. Here is where Internal Controls' implementation becomes fundamental. In fact, the objective of chapter two is to analyse the Internal Control's system and its role as a management supporting tool to prevent fraud. Through the definition provided by the COSO body, the chapter will analyse each element of the framework issued in 1992, focusing also on the *Enterprise Risk Management*, a revisited supporting framework. To conclude, the last chapter will introduce a concrete example of Fraud scam occurred within one of the biggest long distance telecommunication companies in the US. In 2001 WorldCom confessed it had overstated earnings by more than $3.8 billion. Through the analysis of the fraud scheme pursued by CEO Bernie Ebbers, the chapter will highlight how all the concepts introduced in the first part of the paperwork are deeply interrelated. In fact, the scam is a perfect representation of how the lack of internal controls and the failure of corporate governance have been the key drivers of this important fraud scheme.

Contents

TABLE OF FIGURES

Introduction

Today Fraud represents a global problem that affects organisations worldwide and still occupies the headlines of the most important business newspapers. The amount of money lost to occupational fraud each year poses a significant threat to our global economy. It directly impacts the entities' ability to produce goods and services, to create job places and to provide public services. In addition, considering that a significant portion of fraud cases go unnoticed and unreported, the damage could be exponentially higher. In order to deal with such a problem, it is fundamental to have a better understanding of the root causes of fraud so as to improve detection, prevention, and investigation of the phenomenon. For this reason, this paper begins by offering a comprehensive overview of the origins of fraud, with a specific focus on the different theories that have set out to identify the push and pull factors leading to fraudulent behaviour. Many have been the contributions related to the understanding of the concept of fraud, and even if they differed in the methods or in the approaches used, they have all been useful to identify logical links, in order to provide simple and schematic explanations of the elements responsible for the recurrence of the phenomenon. In particular, one of the major contributions in the field of fraud examination was introduced by the famous criminologist Donald R. Cressey and still now it represents the most widely recognised basic framework of fraud. The author realized that each time a fraud scam occurred three key elements were simultaneously present: pressure, opportunity, and rationalization. These three elements have become known as the "Fraud triangle". As Cressey's "Fraud triangle theory" suggests, satisfying needs is not always so immediate as it seems since sometimes, their characteristics makes them difficult to achieve. Therefore, the inability to solve problems by legitimate means, coupled with a continuous sense of pressure is what motivates people to commit crimes in the first place. For instance, in a perfect world there would be no insurmountable obstacle and companies would be able to show positive financial pictures, by meeting both internal and market expectations, without any problem. Unfortunately, this is not the case. When results do not fulfil expectations there may be several reasons for companies to indulge into illicit behaviours. Therefore, the paper will outline and group the major potential incentives for fraud into four main categories: personal incentives, market incentives, special circumstances and cover up fraud.

The focus will then be placed on fraudulent actions which have been defined to be the result of pre-meditated processes. If on the one hand, analysing past events represents a good starting point to understand the schemes used by fraudsters to commit illicit actions, on the other, it does not offer any insight on the concealment strategies used, considering that all past cases have already been detected. Regardless, looking at past strategies is a good way to understand, even if very roughly, some of the dynamics that take place when fraudsters try to conceal their projected actions and can be useful in understanding the characteristics of both individuals and organisations. About this, Fraud cases can be subdivided into three macro areas defined as Asset Misappropriation, Fraudulent statements, and Corruption. Each category will be analysed with the support of data and information on worldwide fraud scams collected by the Association of Certified Fraud Examiners in their 2020 Report to the Nations.

As a consequence of several scams occurred in the late 80s in the US, in 1992 the Committee of Sponsoring organizations of the Tredway commission issued the COSO report *Internal control – an Integrated Framework (IC-IF)* with the aim of providing a clear definition of control and standard as reference for those companies willing to implement sound internal control systems as a prevention tool. There was an urgent need to improve the quality of companies' financial reporting by setting the focus on corporate management, ethical standards, and internal controls. The second chapter will then introduce the concept of internal control focusing also on the evolution of its role from a legislative perspective. Moreover, particular attention will be given to the ERM framework, which represents a reinterpretation of the concepts expressed within the original IC-IF paperwork, emphasising the concept of risk assessment as a precondition in order to plan sound internal control systems. Each of the eight components of the framework will be then analysed to have a complete understanding of the ERM's role within companies.

In order to better appreciate the topics introduced in the first part of the paper, chapter three will focus on WorldCom's fraud case. The latter represents a concrete example of a financial statement fraud in which the three elements of Cressey's Fraud Triangle, Pressure, Opportunity, and Rationalisation, play a significant role. The combination of the three led to the manipulation of financial results in two main ways. First of all, in 1999 and 2000, the company reduced operational expenses by improperly drawing its reserves, also known as "Cookie jar reserves". Secondly in 2001 and early 2002, the entity improperly represented operational expenses as capital assets. Neither of the two methods complied with the GAAP

(General Accepted Accounting Principles) and neither of the two methods was disclosed to investors even if they represented changes in previous accounting treatments. However, both methods contributed to decrease WorldCom's expenses, while artificially increasing its financial statement's revenues from 1999 to the first quarter of 2002. The scam is also a perfect representation of how the lack of internal controls, which has often been reported by the company's Internal Audit department, and the failure of Corporate Governance, have been the key drivers of this important fraud scheme. Analysing WorldCom under a COSO magnifier is helpful to give a in hindsight examination of the fraud case and to explain how it occurred. Furthermore, the analysis of WorldCom under the COSO framework, coupled with the aftermath of the scandal will allows us to reflect on the effectiveness of the measures and the models introduced in the fight against fraud.

1 Chapter 1- Fraud Environment

Launched in 1996 the "Report to the Nations" is nowadays one of the best sources of information about occupational fraud. The Association of Certified Fraud Examiners (ACFEs) annually publicises data collected from thousands of fraud cases occurred all over the world, with the aim of studying the costs and the effects of the phenomenon. About this, evidence suggests that between January 2018 and September 2019 fraud cases amounted to 2,504 from 125 different countries, causing total losses for more than 3.6 billion dollars, with an average loss per case of $1,509,000. In addition to this, Certified Fraud Examiners (CFEs) estimate that organizations suffer losses of 5% of their revenues to fraud each year. Of course, this is just an estimation. However, it is worth considering that not all fraud cases manage to be discovered and reported. This is why the damage caused by the phenomenon could be even greater. By the way, even if the next chapters will focus on fraud within companies, in order to deal with such a huge problem, which still undermines our economy to the point that organizations continuously suffer important losses from it, it is essential to first understand how fraud developed through the centuries. In fact, it would result superficial to just stick to the most recent episodes thinking that such scandals only belong to the last few years. Therefore, what is the origin of Fraud?

Fraud is not a new concept, rather it dates back to the first years of trade where individuals, some of whom were already interested in obtaining superior gain in respect to their counterpart, exchanged all types of resources from spices to precious metals. In regard, the very first episode happened back in 300 B.C. when a Greek merchant, named Hegestratos, subscribed an insurance policy in order to leave the port with its ship and sell the corn he was transporting. The arrangement known as *bottomry*[1], granted him the money to travel, using the ship as a collateral. However, once the merchant completed the delivery, he should have been supposed to pay back the loan, otherwise the lender would have been authorized to claim both the cargo and the money back. In order to keep both of them, Hegestratos tried to sink the empty ship, but he was caught during the operation by some members of the crew. Evidence of fraud concept recurred also in Hammurabi's code, one of the earliest sets of laws, dating back to 1760 B.C. Precisely, law 265 stated: "*If a herdsman, to whose care cattle or sheep have been entrusted, be guilty of fraud and make false returns of the*

[1] Terminology used in maritime transactions where the owner of a ship borrows money and uses the vehicle as a collateral.

natural increase, or sell them for money, than shall he be convicted and pay the owner ten times the loss". However, despite the fact that ancient civilizations had already considered them as acts which deserved punishment, in the first years of the '80s, society was actually indifferent to fraud crimes, rather considering them as acts which lacked violent behaviour and which, for this reason, were proper of brave men. This led people to show a sort of admiration for individuals who were able to indulge in fraud. Recently though, people's perception about the situation has changed significantly towards greater awareness of the gravity of illicit actions and greater concern with the methods of prevention, which have been continually criticised to be poor and ineffective. Talking about illicit actions, three types have been identified: extorsion, theft and mystification. Fraud belongs to the theft category which is also recognized as the less harmful among the three. However, the term has not been easily defined and also many scholars struggled to find an appropriate definition, probably due to the incapability of using specific and accurate terms, while having to rely just on slang or generic ones to define a broad legal concept. Black's Law dictionary, 7^{th} edn (1999) defined fraud as *"A knowing misinterpretation of the truth or concealment of a material fact to induce another to act to his or her detriment*". Even if the definition slightly changes when moving from country to country, there is a general consensus that fraud involves breaking the law and working outside the regulatory framework. This is especially true when setting the spotlight on the Financial Statement Fraud, which is a subset of fraud in general, that enables to analyse the phenomenon within organizations, where the main actors are individuals or management teams. For what concern individuals, their involvement is generally related to theft of cash or inventory while for management it generally relates to the redaction of false financial statements in order to distort reality. What is particularly intriguing about Fraud, is that it can surface almost anywhere without making any distinction, from big to small companies, from old to new companies, from manufacturing to service ones and from public to private. An insight of this is given by the histogram publicised in the 2020 *Report to the Nations* which represents the five types of organizations victimized by occupational fraud, showing for each of them the percentage of identified cases as well as the median loss. Clearly, the highest percentage of cases occurred in private companies, followed by public ones, while just 9% occurred in Non-profit organizations. However, the weight of the median loss of $75,000 should not be underestimated, considering how devastating this loss could be for a category which generally faces greater issues, with respect to the others, in raising money.

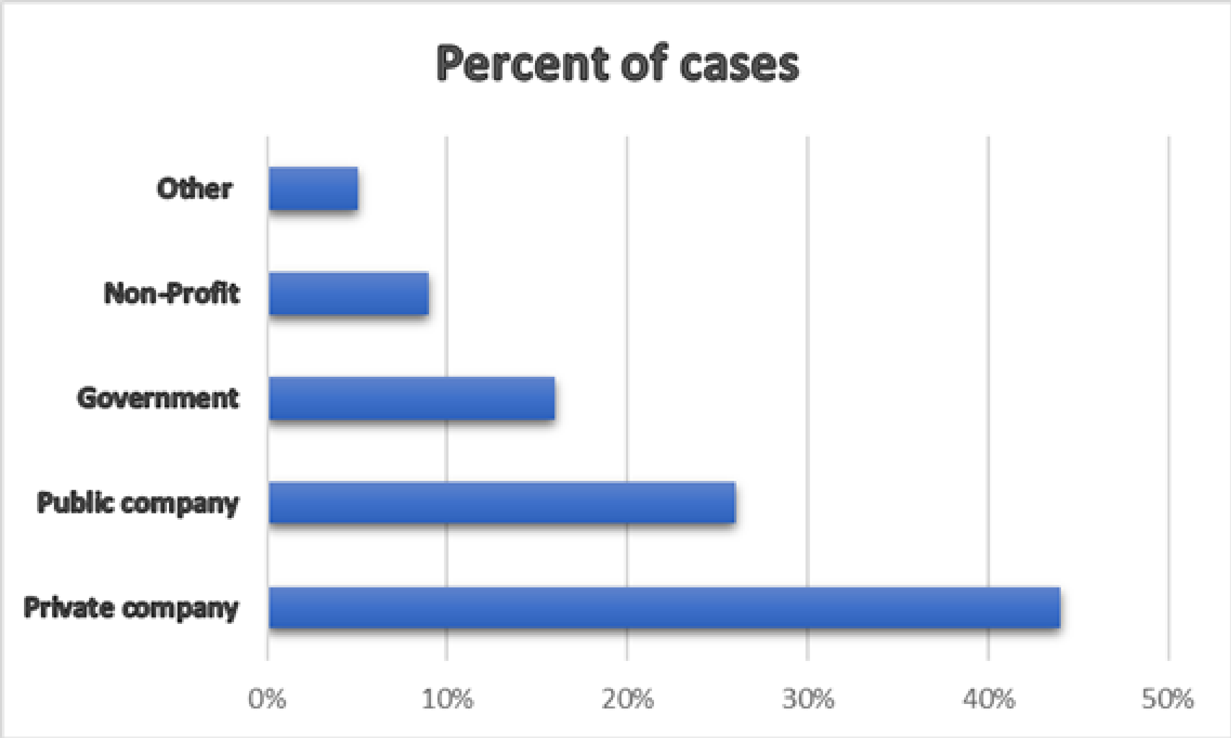

Figure 1"What type of organizations are victimized by occupational fraud?" (Source 2020 Report to the Nations)

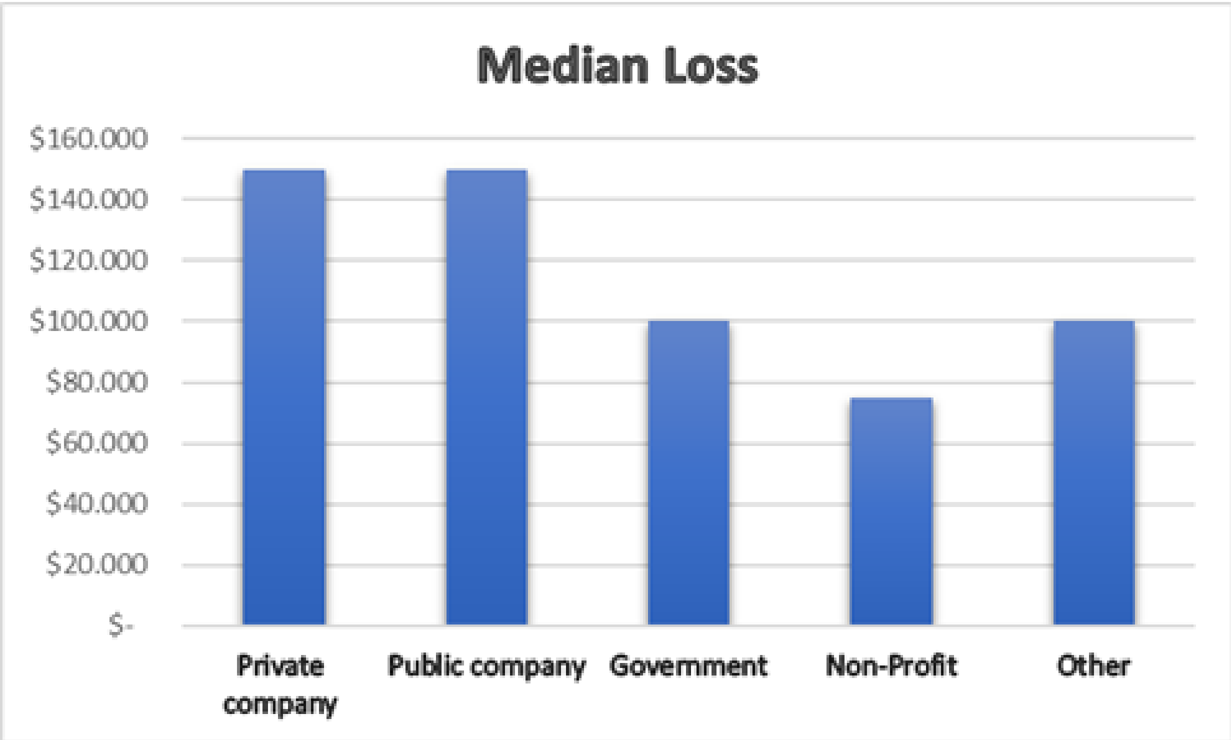

Figure 2"The median loss for each type of victimized organization" (Source 2020 Report to the Nations)

To conclude, fraud has always been present during human beings' lifetime and through all over the eras it has been subject to different and evolving opinions. However, the reason why today fraud crime is perceived to be exponentially increasing is a consequence of society's major interest in the matter and also matured awareness of the dangerous repercussions the phenomenon can have.

1.1 At the root of illicit conduct

Over the years, many studies have tried to explain and identify the origin of crime in general, focusing especially on a particular subset of crime, Fraud, which still occupies the headlines of today's most important business newspapers. Scholars have gone way beyond the rational theories developed in the late 19th century by the two well-known philosophers Cesare Beccaria and Jeremy Bentham, suggesting that criminal behaviour is not linked to rationality, rather it involves emotions. Starting from here, many studies have tried to concentrate their resources on understanding the causes and the conditions to indulge in fraud. Interestingly, sociological theories completely dissociated from the rational ones, recognizing that criminal behaviour is instead a combination of both subjective and contextual elements. The former involved characteristics such as self-esteem, emotions, intelligence while the latter referred to social control and belongingness need. Great evidence has been provided by the "General Strain Theory" developed by Robert Agnew[2] , who identified the presence of a negative feeling coming from individuals who realised they were not appreciated or valorised from the society to which they belonged as they would have wished to. This tension could have easily brought individuals to indulge in illicit actions with the aim of improving or changing the actual situation, especially if they had failed to achieve objectives which the society believed to be important such as money, status, and autonomy. In addition, the less self-esteem an individual had, the greater his strain perception would have been. Therefore, the theory supported the idea that committing crime was not an immediate and rational choice, but rather an individual's incapability to control emotions.

In the first period of the '90s, Emilie Durkheim[3] introduced the concept of *Anomie*, literally a break in the normative system, which she identified to be the principal cause of illicit behaviours. At that time, industrial society was indulging in hyperstimulation of people's aspirations, that led individuals to falsely believe they could enhance their status and achieve their personal goals. The problem was the presence of strong controlling systems, which limited the aspirations of the different social groups. Of course, in the long run, this generated a collective status of impatience, which resulted in a behavioural deviance from norms, since it was perceived as the only way to overcome the obstacles that separated individuals from

[2] Agnew R., "Foundation for a General Strain Theory of crime and delinquency", in *Criminology*, vol. 30, N. 1, 1992
[3] Poggi G., *Emile Durkheim*, Il Mulino, Bologna, 2003.

the achievement of their desired goals. Several other theories tried to elaborate an answer to the issue and some of them were even in contrast, not a surprise, considering that the item of the study was the human being's behaviour which is strongly influenced by many subjective components. This is why there was no wrong or correct theory but rather all of them are still useful to provide a better understanding of the matter and to encourage further analysis. One of the major contributions in the field of economic crime, that also inspired following authors, was given by the criminologist Donald R. Cressey[4] in 1953. His work consisted in an interview to two hundred individuals who had been indicted for misappropriation, with the aim of creating a model that could explain the reasoning behind illicit actions. His findings are still now the starting point used by auditors or CFEs to cautiously identify any fraud case within organizations. The author realized that fraud was not a casual event rather, when it occurred, three main elements were always simultaneously present: *pressure*, *opportunity* and last, but not least, the *rationalization* of the action. The theory, better known as "The fraud triangle", places at the very top vertex *pressure,* which Cressey described to be a status, perceived by individuals, towards a need that it is usually satisfied through their activity. However, at that time and still now though, this is not always so immediate, considering that sometimes needs appear to be difficult to achieve due to their specific characteristics and considering also that *pressure* can appear all of a sudden, thus motivating individuals to break the rules. Interestingly, still now, people facing pressure try to conceal it expressively avoiding for it to become public. In fact, what shames fraudsters the most are the circumstances that cause the behaviour to manifest and not the action itself such that, concealing pressure, permits them to preserve their reputation and to continue enjoying social acceptance. Examples of *pressure* are represented by gambling, excess credit card debt, difficult goals to achieve in the work environment and also unexpected financial needs. At this point though, once the sense of pressure emerges, it is fundamental for the fraudster to believe that his actions will not be detected and that the opportunity to succeed actually exists. What shapes the opportunity force is the combination of general knowledge and technical abilities owned by the fraudster, which are necessary in order to have a good understanding of the organization's characteristics, of its weaknesses and of the inside procedures. About this, poor training, lack of supervision, weak ethical culture, or lack of prosecution of perpetrators are all sources that can increase the perception of an existing opportunity. The most interesting condition of the model, which

[4] Cressey D.R., *Other people's money: a study in the social psychology of embezzlement*, Tree Prees, Glencoe, Illinois. 1953.

also represents the last vertex of the triangle, is represented by *rationalization*, a process through which the individual tries to find a plausible justification to his projected actions, minimizing the impact that these could have and convincing, not only other people, but also himself of his innocence. It is important to point out that *rationalization* is an *ex-ante* process, meaning that it takes place only before the action is pursued, in order to lower the inner sense of guilt perceived by the fraudster, while falsely believing to be the victim. The main way by which individuals tend to justify fraud is to convince themselves that it will be a just one-time thing and that a solution will be provided as soon as possible. This work turned out to be a very important source of inspiration for many other authors which contributed to the model by adding personal and new innovative elements. Regarding this, William Coleman[5] analysed the phenomenon by looking at it from a different perspective and suggesting, for the first time, that also the organization's environment could be perceived as a potential key driver to fraud. In fact, while people usually spend a great amount of time in their workplace, they failed to realize that, in doing so, they quit every kind of relationship with the external environment, creating a form of isolation around them, such that the only thing they care about are the values and the opportunities offered by the organization. Therefore, Coleman suggested that this clear separation between external and work environment enhanced the influence power exercised by the network of social relationships within the organization, towards not only the worker's judgements but also on his perception of crime. To clarify, if an employee works in a company dominated by a widespread idea of non-compliance to the norms, he will end up projecting his work based on such a belief. However, the latter will be judged to be illegal by the external environment. Still now, the corporate environment of a firm is recognised as a fundamental element that contributes to minimize the opportunities of fraud. This is why there should always be a good and sound corporate governance at the top of each company.

Going back to Cressey's contribution, over the years, not only the model has been complemented by different authors with their new ideas, but the "Fraud triangle theory" has also evolved into the "Fraud Diamond Model", thanks to the introduction of a fourth characteristic, *capability*, suggested by Wolfe and Dana Hermanson[6]. According to the couple, fraud could not occur without the right person who possessed the right knowledge and the right abilities to carry it out. Therefore, it was no more a matter of just having an

[5] Coleman J.W., "Toward an Integrated Theory of White-Collar Crime", in *American Journal of Sociology*, Sep. 1987.
[6] Wolfe d., Hermanson d., "The Fraud diamond: Considering the Four elements of Fraud", in *The CPA journal*, dec. 2004

opportunity, but rather of individuals who were able to take advantage of the *opportunity,* transforming it into reality. More of the authors' attention was addressed towards case frauds committed by people occupying high positions within the organization, with a long tenure and with a significant volume of resources stolen from the company. Interestingly, the couple observed that people who were able to recognize the existence of an opportunity, taking advantage of it, also had specific and recurring personal characteristics such as intelligence, ego, persuasiveness, a good position within the organization and also a good ability to manage stressful situations. All of these traits contributed to shape an individual able to use its position of power to exploit opportunities, to understand how to deceive internal control systems, to convince other people to collaborate and to possess a high level of confidence in its actions. Many of the following studies, starting from the '70s, benefitted of the above findings which were based primarily on human's behaviour, on personal social-characteristics and on motivation to indulge in fraud, but they also progressively shifted the spotlight towards organizations – corporate, professional or governmental- as subjects likely to indulge in illicit actions, with a special attention towards their operations in the competitive environment and their structural and cultural elements.

On the basis of this new prospective, in 1970 Herbert Edelhertz[7], head of the fraud section of the US Department of Justice, highlighted in his work the difference between two types of crimes, the *occupational crime,* which occurs when an employee, despite the damage caused to the organization, takes advantage of his working position in order to personally benefit from an illicit action and the well-known *white-collar crime*, committed by the organization in order to benefit as a whole. This progressive and particular shift towards organizations is still present nowadays and it is also subject of deep analysis by auditors and CFEs who have incorporated all the above findings in order to prevent, detect and report all the accounting scandals. Source of evidence is given by the *Annual Report to the Nations,* a work which uses all the previous contributions in order to address the problem. Recalling Wolfe and Dana Hermanson's work for example, CFEs have confirmed the existence of a strong correlation between fraudster's level of authority within the organization and the fraud's size. In fact, in exhibit 1.1 related to the period between 2018-2019, despite the fact that the reported cases for owners and executives amount to just 20% compared to 41% for employees, it is evident how the loss caused by the formers amounts to $600,000 against just $60,000 by the latter.

[7] Edelhertz H., *The nature, Impact, and Prosecution of White-Collar Crime*, National institute of Law Enforcement and Criminal Justice, 1970.

This huge difference can be easily explained by looking at the authoritarian position occupied by owners or executives and to the benefits that this allows them to enjoy. For instance, having access to all the resources of the company and, at the same time, to all the assets, guarantees them a position of privilege with respect to their lower counterparts, causing grater damages to the organization.

Overall, many have been the contributions related to the understanding of the fraud concept, but it's worth highlighting how, even if they differed in the methods or in the approaches used, they have all been useful to identify logical links, in order to provide simple and schematic explanations of the elements responsible for the recurrence of the phenomenon.

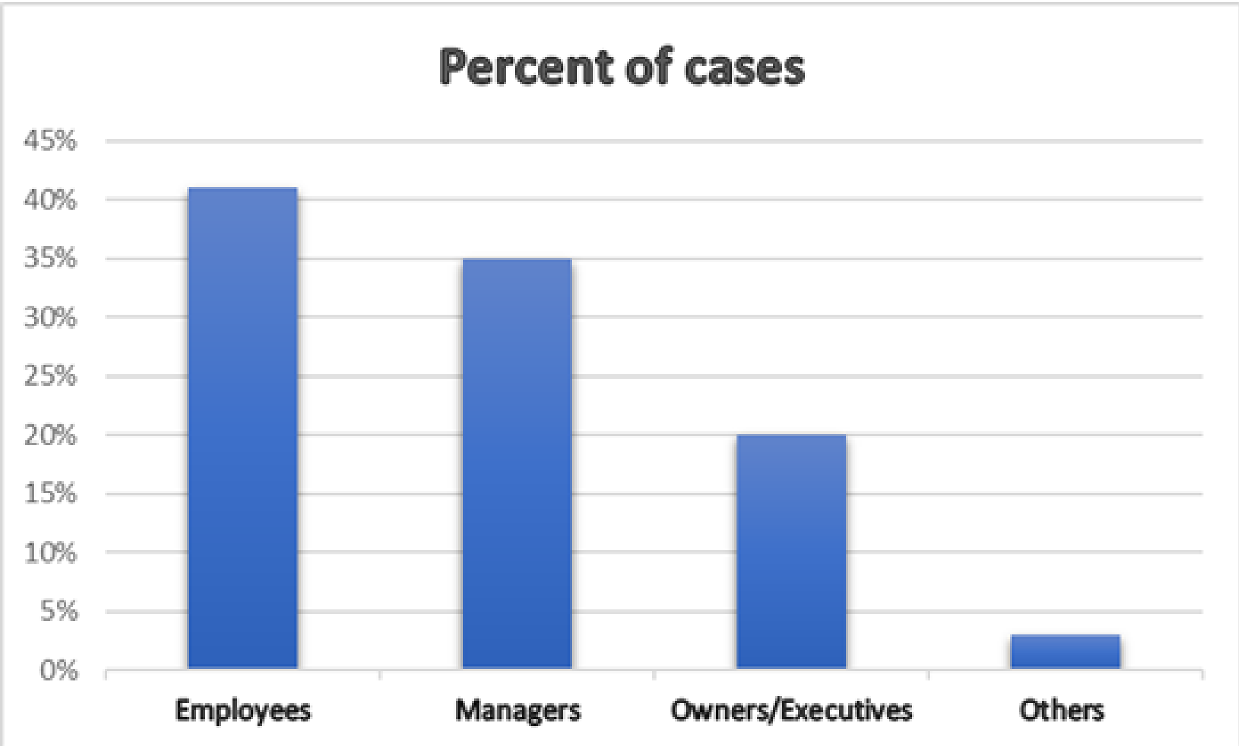

Figure 3 "How does the perpetrator's level of authority relate to occupational fraud?"(source 2020 Report to the Nations)

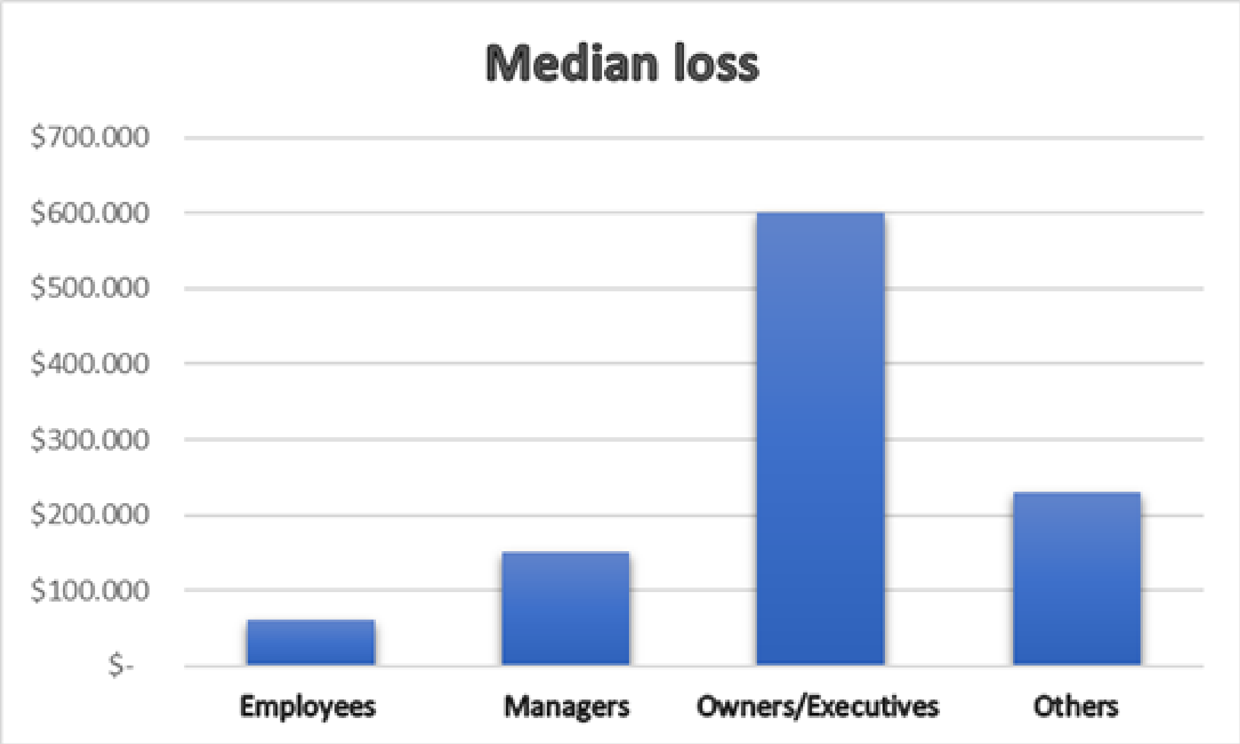

Figure 4"The median loss caused by the perpetrator's level of authority" (Source 2020 Report to the Nations)

1.2 Conditions to indulge in fraud accounting

As Cressey's "Fraud triangle theory" suggested, satisfying needs is not always so immediate as it seems since sometimes, their characteristics makes them difficult to achieve. Therefore, the inability to solve problems by legitimate means and the continuous sense of pressure is what motivates people's crime in first place. Similarly, this is what happens within organizations where, instead, meeting expectations is not always that trivial. For instance, in a perfect world there would be no insurmountable obstacle and companies would be able to show positive financial pictures, by meeting both internal and market expectations, without any problem. Unfortunately, this is not the case, considering that some organizations struggle to show profits and have to survive to persistent financial distress conditions. Once again, pressure is what motivates crime in first place. A common incentive for companies that face financial difficulties, will be to report higher profits by increasing fictitious sales, increasing net assets while at the same time reducing debt and liabilities. However, this is not universally true, since many companies could find themselves in a completely different scenario where conversely, it might be more prudent to decrease profits in order, for example, to divert the government's attention, especially when dealing with regulated industries which are subject to governmental price controls. In fact, in this specific case, what companies fear the most is that, by showing a rosy picture of the organization and by reporting high profits, the government could intervene by fixing their prices, or also profits, in order to contrast the excessive profit making.

Stated this, what is now fundamental to underline, before moving to the incentives' analysis, is that contrary to what is the common thought, Fraud is not an immediate event, rather it usually begins with the use of Creative Accounting techniques. However, before entering deeper into this specific concept, it is an initial prerogative to first understand the role of the regulatory framework in which companies operate, since it will be the turning point in order to appreciate the differences between Fraud and Creative Accounting. Therefore, the regulatory framework, which differs from country to country and that accordingly might include international standards, national standards, company law (especially in some countries of Germany and UK) or also independent accounting commission, has been introduced in order to issue regulations as well as accounting principles, which all companies should follow to present a "true and fair view" to all the users of such information. Established this, it is now worth moving to the concept of *creative accounting* which is a well-known term that has created and still creates, widespread disagreements and contradictions in relation to its definition. In this regard, USA for example, combines Creative Accounting and Fraud into a unique issue while, on the other hand, UK strictly differentiates them and accurately defines Creative Accounting as a method which uses *flexibility* within the regulatory framework. Substantially, Creative Accounting takes advantage of the gaps existing in the accounting principles, with the aim of serving the preparator's interest instead of the user's one. Since not all companies operate in the same environment and not all of them pursue the same strategies, *flexibility* is particularly necessary for listed companies, during the financial statement preparation, in order to present a "true and fair view" of the accounts. Therefore, if flexibility ceases to exist, then also the "true and fair view" principle would accordingly fail to exist and this would go to detriment of people interested in the company's investments or, more generally, of shareholders interested in evaluating whether to buy, sell or hold shares of the company and that take their economic decisions on the basis of the information reported on the financial statement. This scenario offers a favourable incentive for managers, who are responsible of the financial statement preparation, to use *flexibility* during the reporting process so that the accounts will manage to comply with the regulation, reflecting a "true and fair view". The Chartered Institute of Management Accounting (2000), *official terminology* defined the term as "A form of accounting which, while complying with all regulations, nevertheless gives a biased impression (generally favourable) of the company's performance". Therefore, using creative accounting is not considered as a breakthrough the law because it is still a method pursued within the regulatory framework, even if it diverts from the basic purpose of accounting, which is centred on providing users with a "true and fair view". Understanding this concept is far important since it represents the very first step before fraud is committed. About this, generally, a typical scenario involves a company having to face a poor yearly result, as a totally unexpected performance. The immediate reaction of the management team in order to fix the bad result and show a better condition of the company, is to start using Creative Accounting, with the hope that next year's result will meet the expectations and that there will be no further need to indulge in other adjustments. However, when the next year's results will turn out to be even worse than the previous ones, causing greater pressure on the management team, the latter will be incentivized to use extensive creating accounting techniques in order to portray the accounts in a light favourable to themselves, once and for all. At a certain point though, by continuing to operate within the regulatory framework, it will become quite impossible to show further positive results without having to violate the law and finally indulging into Fraud.

Once stated that generally fraud immediately follows creative accounting techniques, it becomes fundamental to deeply analyse the motivations to indulge in such behaviours, to the point that the major potential incentives have been grouped in four main categories in order to offer a clearer view: *Personal incentives*, *Market expectations*, *Special circumstances* and *Cover-up fraud*. However, if on the one hand this subdivision offers a broader overview of the main reasons to indulge in fraud, on the other, in the real world, it is not so helpful in order to determine which of them has actually contributed to be the key driver to managerial actions. In fact, to disentangle the right incentive it is hard work. Regardless of this, under the *personal incentive* category, five specific incentives have been identified: "Increased salaries", "Bonus-related pay", "Shares and share options", "Job security" and "Personal satisfaction". Even if these incentives are treated separately, they all share the ability to tempt managers to indulge in creative accounting or Fraud, since they all directly benefit from them. In fact, it is not a mystery that, managers or, indifferently, directors are rewarded if they manage to achieve the targets imposed by the organizations for which they work. Additionally, for every specific objective achieved they also receive a bonus, which is defined as the variable part of a worker's remuneration to be added to the fix part of the salary.

Considering that all managers have the ambition to obtain a bonus and to improve their economic condition, they will clearly be incentivized to indulge in creative accounting or fraud to show positive results, even if actually there is no correspondence with the truth. Regarding bonuses, some studies have demonstrated that in order for them to be considered effective, they should affect the fix part of the salary for a percentage between 5%-10%, otherwise the risk of going beyond 10% would lead the worker to be too focused on the quantitative part of the incentive rather than on the qualitative part of the work. Substantially, the desire to achieve a very high bonus could represent a solid motivation to manipulate the accounts. By the way, it's not always about cash, rather what commonly happens within companies is that directors, or more properly CEOs, especially in strong equity markets such as UK and USA, receive share options as an alternative form of remuneration. This technique offers them the possibility to acquire shares of the listed company at a settled price. Therefore, since share's performance depends on several factors, both internal and external to the organization, with profit being the main driver, if a company reports high profits accordingly, its share price will increase, while the opposite happens if unfortunately, the company performs poor results. As directors benefit directly from increases in salaries, they will surely be incentivized to use any method, legal or illegal, to make sure that the company achieves good profits. Contrary to the above-mentioned incentives, *job security* and *personal satisfaction* instead, are more focused on the human part of managers. In fact, by reporting disappointing results managers could feel not only vulnerable and at risk but also, they may lose self-esteem which will certainly impact on their personal satisfaction and on the company as a whole. To avoid all this, managers may decide to illegally drive-up profits, showing a perfect and positive picture of the company.

The second category, defined as *Market expectations* includes three main incentives which might represent the key drivers for companies to act illegally in order to give positive signals to society. Here, the concept of *market signalling* becomes really important especially if considering the impact that the receiver's signal interpretation and the receiver's reaction alternatives can have on organizations. In this regard, the first incentive, represented by *Meeting analysts' expectations*, is what matters the most for companies, such that analysts are considered to be the very first important receivers of companies' signals. Ordinarily, companies which meet certain criteria, such as being listed, for example, must cyclically report their information in a formal way both on an annual basis and interim basis or rather occasionally on a quarterly one. Based on the available information and also on companies' present data, analysts will make accurate assumptions on companies' future profits, thus delivering a very helpful tool to investors and stakeholders, who generally share an economic interest in companies, to get an idea of how they will perform in the next years. At the same time though, since companies' share price is the reflection of analysts' projections, the strong relation between the two delivers great power to the analysts' role and especially to their findings. Stated this, the huge problem arises if a company is not able to live up profits to meet analysts' expectations, on which both the market and society firmly rely. In fact, disappointing results will undoubtedly lead to a share price suffering, which accordingly will represent a big issue for directors whose remunerations are related to the company's share price. As a consequence, directors always feel a great pressure on meeting analysts' forecasts at the point that, in case of a shortfall, they might surrender in creative accounting techniques or worse-case scenario in fraud.

A second pressure that companies might face in the real world is the need to indulge in *profit smoothing,* since by releasing steady profits, the company will be perceived as less risky by the market. Just to clarify the concept with a simple example, let us consider two companies X and Y. Suppose X doubles its profits every year such that it keeps reporting positive results, while Y makes the same profits as X over the years, but in a more irregular way, jumping too easily from positive to negative results.

(Numbers expressed in £m)

Company	Year 1	Year 2	Year3	Year 4	Total
X	2	4	8	16	**30**
Y	20	-5	10	5	**30**

Figure 5 "Illustration of Profit smoothing"

Surprisingly, as the table shows, computing X's and Y's profits leads to the exact same result: thirty. Even if the final total number is the same for both of them, there is a huge existing difference between the two, which is identified in the trend of their profits. In fact, having steady profits that double every year will help analysts to make better projections for the company's future results, which accordingly makes the market more comfortable and increases its trust on the target company. This is why Company X will always be perceived as less risky while instead company Y will always be perceived as erratic and less well managed. Undoubtedly, this negative perception will influence the organization's share price, leading it to less predictable swings. However, a weak share price is not just a bad signal for society, but it also represents a big threat in the eventuality of a takeover, since it would be much easier for a sound company to acquire the one facing share price difficulties.

For such reasons, managers might be incentivised to adjust profits and to show a stable situation of the organization they are working for, avoiding both possible takeover bids and remuneration decreases.

The third category goes under the name of *special circumstances* which comprises a range of different situations that might incentive managers to commit illicit actions. A typical scenario is when a company borrows a certain amount of money in order to run its operations or alternatively to invest it. As expected, lenders (for the majority banks) will be willing to have their money back as soon as possible. Therefore, to make sure that the company will be able to repay the entire amount of the borrowing, together with the matured interests, they will set up some covenants, that are nothing different then conditions to which the company should not breach. What often happens is that companies and lenders mutually agree to set a so-called *gearing level*, which is an indicator highlighting how much of the companies' operations are funded through debt and how much through equity. In fact, by setting a *gearing level,* lenders try to protect themselves from company's exceeding their debt size and defaulting immediately after it, with the risk of being left empty-handed. Therefore, if the company borrows too much and for this reason it breaches the settled *gearing level*, the entire loan must be immediately repaid back. To avoid this kind of situation and to continue to benefit from the loan, directors might be motivated to use an OBS, also known as *off-balance sheet* technique, which consists in not including a liability, thus using account's manipulation to remove part of the debt and to avoid the covenant breach.

Still within the same category, companies might indulge in fraud also when motivated by *new issues,* such as entering the stock market for the first time or collecting more money from a share issue. About this, in both situations, giving a good image of the company's profitability will increase trust in it. By doing so, the company will be perceived to be a sound entity and more shareholders will be willing to subscribe its shares, thus influencing the share price, which will respectively increase. Accordingly, a higher share price will lead to a higher amount raised by the new operation. As a consequence, then, the company will do anything in order to show a positive picture and good results, even surrendering to Fraud.

Another typical scenario regards companies involved in special operations such as *Mergers and Acquisitions* (*M&As)*. In this case, whether the company acts like the target or the bidder, it is still incentivised to indulge into Fraud. Regarding the Bidder's position, it is actually important for him to have a strong influence over the operation. In fact, what usually happens is that the bidder offers as part of the purchase price some of its shares to the target company. If the Bidder is doing well, meaning that it is profitable, also the share price will reflect this condition and the higher the share price will be, the less shares the company will have to offer to the target one. "Research showed that in the late 1980s in the UK one very acquisitive company, Hanson, launched 16 takeover bids. Only one was launched when the share price of Hanson was comparatively weak" *(Mansell, 1987).* Mansell's statement confirms the above reported concept, highlighting how share's price strength actually matters during the involvement in special operations and how it dictates the perfect time for the launch to take place. On the other hand, from the Target perspective, showing a picture better than it actually is, definitely forces the bidder to offer more in order to complete the acquisition of a sound company. At the same time though, pretending to have good results could also help the company to stand out and contrast a hostile takeover bid. Once again, despite being the bidder or the target, manipulating the financial statement by increasing profits would be a quick and simple way for both parts to succeed in an M&As operation.

An Additional threat, when operating in the market, is represented by the interference of the government through its regulations. In fact, companies' reporting high profits fear a regulatory intervention which could badly affect their selling prices by fixing them down to a certain level or by introducing windfall taxes, which are tariffs specifically addressed to organizations that have benefitted from economic expansion. This is why many companies operating within the market, such as water companies or oil companies, will try to avoid making high profits or more easily, they will cook the books by using income decreasing policies in order to divert the government's attention.

Within the *Special circumstances* category there is also the so-called *Big Bath* policy. As usually reported in the news, it's typical for an organization to change its management team during the years of activity, especially when the company is not achieving the desired goals. What is even more typical, is that the upcoming management team, in order to meet the internal and market expectations, will show an even worse scenario of how the company was doing before their intervention. Clearly, the aim is to show how the contribution of the upcoming team has quickly changed the company's poor results and it also permits them to start working from a lower basis, making it definitely easier to raise the bar. Therefore, in order to show that the choice of having them as executives was the correct one, the new team will be incentivised to manipulate the accounts by making, for example, immediate provisions for expenses that will be suffered in the future, such that future expenses will be reduced while, accordingly, future profits will be increased.

The last category, *cover-up fraud,* usually takes place when a misappropriation of assets has already occurred. In order to cover up the illicit action, managers are incentivized to indulge in fraud through the manipulation of the accounts, made outside the regulatory framework.

To conclude, evidence shows that living in a non-perfect world can create several though situations where managers or directors of the organizations, as a reaction, might be incentivized to indulge in illicit procedures in order to fulfil external or internal expectations. As the paragraph highlighted, the main reasons could be part of a range of *personal incentives*, therefore of directors willing to increase their personal remunerations, for example. Alternatively, they could be due to the pressure to meet the *analysts' expectations* or also to other *special circumstances,* such as the introduction of a new management team, the launch of M&As operations, the emergence of new issues and finally, as a way to cover-up a misappropriation of assets. The detailed description of all four categories is functional to understand how the temptation for fraud can actually arise from very common and simple situations and that, for this exact reason, all of them should be deeply monitored when happening, since they could represent a first important red flag before manipulation actually takes place.

1.3 Overview of fraud categories

As highlighted in the previous chapters, fraudulent actions have been defined to be the result of pre-meditated processes. In fact, such actions generate pre-ordered schemes, that are considered to be the means through which perpetrators pursue their illicit actions. Therefore, based on such definition, fraudulent actions are clearly not driven by impulsive instincts, rather they represent the result of precise schemes which main focus is to find the most effective way to conceal such activities. Of course, the final aim of fraud schemes, is always to cover something illegal through the presentation of an apparently legal form by taking advantage of the opportunities recognised within the enterprise. The latter are strongly related both to the role held by the perpetrator within the organization and also to the emerging weaknesses of the victim company. Therefore, schematization, concealment and opportunity are three of the most important elements to identify and to analyse when fraud scams take place, rather than personal elements which are strongly related to the individual's psychology and to his personal sphere such that, for this specific reason, they are more difficult to detect. This is why scholars have concentrated their resources in analysing elements which could be observed objectively, such as the three elements previously mentioned. For instance, analysts observed all detected fraud scams in order to treasure all past experiences and, at the same time, to collect all possible information about the phenomenon. In fact, looking at data collected, it is common thought that, the majority of fraud cases occurred following certain consolidated and repeated schemes. In fact, it is not a mystery that fraudsters are considered to be brave individuals who possess high capabilities and high doses of creativity, but by going in depth, it emerged that these qualities are not applied in the projection of schemes rather, they emerge during complementary concealment processes. Of course, the final aim is to disguise the real intention of perpetrator's actions. For instance, by analysing a particularly well-known type of financial fraud, such as the Ponzi's scheme, it is interesting to notice how, there is nothing so sophisticated behind this strategy, since the fraud scheme followed an extremely easy logic which everyone could comprehend. What instead led to the perfect functioning of the scheme was the great ability to conceal such strategy. About this, the scheme provides for the promise of high returns on short-term investments. This is how the perpetrator manages to attract investors. In order to pay those returns, instead of truly investing the money received, the fraudster relies on the funds paid by other new joiners, who are attracted by the proposal of obtaining superior gain. Since first investors truly receive the promised returns, then other new joiners will be willing to participate, thus establishing a sort of spiral, which in the long run will be destinated to collapse. In fact, this system works well if many new joiners engage in it, or else, at a certain point the collected capital won't be sufficient to repay all the investors, thus leading to the fraudster's escape together with all the money. Alternatively, competent authorities could manage to detect the premeditated financial structure and put an end to the fraud. This is a typical example of a very elementary scheme attributed to Bernard Madoff, the USA entrepreneur, that has been recognised to be the protagonist of one of the major financial scandals in the history. Despite having been revealed, this strategy is still used nowadays to fool investors. Hence, in the past, these scams had determined the urgency to systematically collect all evident data on fraud schemes, since analysts believed them to be more objective and efficient with respect to data acquired by studies on human behaviours and human's motivations. In fact, the latter were considered to be more difficult to observe due to their subjective nature. Therefore, the final aim was not only to report all the information acquired through fraud schemes' analysis and to classify fraud in homogenous categories, but also to point out all the concealment methods used by perpetrators in order to have a clearer view of the phenomenon. However, the attempt to homogeneously classify all the cases into a proper category hasn't been so simple. About this, the existing differences within classification methods and the nature of the phenomenon, which is known to be characterized by a multitude of different elements, made it very difficult to include all cases in just one particular category. For such reasons, the idea of finding the right way to group fraud scams has given way to the collection of different types of information such as the operations, the behaviours and all the common elements that are implemented in fraudulent actions, in order to find the ones recurring in all situations. In fact, the latter could possibly lead to a sort of delineation of a predefined model. Therefore, despite the type of fraud classification model used, prevalence is given to data collected from previous cases, since they can represent a useful tool for those whose aim is to contrast this criminal phenomenon. However, if on the one hand, this model is useful to draft a scheme in order to understand where actions take place, on the other, it doesn't give any insight on the methods of concealment used by fraudsters. In fact, as previously said, the great level of creativity possessed by criminal individuals emerges during the process of action's concealment. For instance, going back to the Ponzi's scheme example, it is worth highlighting how the concealment methods used by Charles Ponzi and, ten years later, by Bernard Madoff were totally different. This comparison is nothing than a confirmation to recent findings, which suggest that concealment strategies are not easy to schematize, since they are influenced by too many existing elements, such as the fraudster's personal characteristics, its capabilities to take advantage of the opportunity, its position within the organization, but also by the organization's characteristics and the processes that rule its activities. It is clear that this strong influence with such subjective elements, makes it very complicated to represent a homogeneous category which is able to comprise similar concealment strategies. In addition to this, it is important to highlight how, the reason why some fraud cases have been successfully implemented, is mainly due to the fraudster's great ability to conceal the illicit actions in many sophisticated ways. Therefore, if on the one hand, analysing past events represents a good starting point to understand the schemes used by fraudsters to commit illicit actions, on the other, it is not so useful to better understand the concealment strategies used, since all past cases have already been detected. As a consequence, the perpetrator's methods have not been very effective. This is not to say that analysing past events is worth nothing, rather this should be used to make people, who rely on these data, aware of the dynamics of the topic, avoiding them to approach the information in the wrong way. Still, looking at past strategies is a good way to understand, even if very roughly, some of the elements that take place when fraudsters try to conceal their projected actions and they are also important to give major attention to some individual's and organization's characteristics.

About this, the already mentioned 2020 Report to the Nation, follows the above structure by deeply analysing fraud cases which have occurred all over the world, focusing on a narrow segment of fraud: the occupational fraud. Within the report, fraud cases are categorised in three macro areas: Asset Misappropriation, Fraudulent Statement and Corruption which in turn are subdivided into further sub-categories that, due to their graphical representation, which recalls the shape of tree branches, are also known as “fraud tree”. Going by steps, the first category is defined as *Asset misappropriation* and it includes all fraud cases that involve a theft of money, assets or of any other valuable resource for the organization committed by an employee, with the aim of increasing its personal gain to the company’s detriment. As the 2020 report to the nation highlights, this category is the most targeted by fraudsters. In fact, evidence shows that the detected cases occurred within the period between January 2018 and September 2019 accounted to 86%. However, at a first glance, it is impossible to not notice how, the median loss caused by the same category amounts to just $100,000, which is a relatively small number if compared with the one related to the loss caused by the other categories. Essentially, even if evidence suggests that Asset misappropriation is fraudsters’ most used and preferred scheme, it is actually recognized as the less harmful one for organizations. In line with the tree fraud, the second category is represented by *Fraudulent statements*, which comprises all cases related to financial statement manipulation. The scheme is pursued through the alteration of financial documents or by the concealment of important enterprises’ quantitative-qualitative information. Interestingly, evidence from the 2020 Report to the Nations, highlights how cooking the books amounts just to 10% of the detected cases, which is far below the Misappropriation of asset’s percentage. However, despite this, the median loss caused by this scheme is respectively $954,000, which suggests how harmful the repercussions of these actions can be for victim companies. Finally, as part of the last category of the Fraud tree, *Corruption* comprises all cases in which, during a business dealing, an individual takes advantage of his position in order to obtain, usually, personal benefits, but also sometimes, to obtain them in favour of other colleagues by going against the principles of its mandate and also against third party’s rights. Such actions include promises, bribery, economic extortion, collusion as well as a wrongful use of pressure exercised towards important exponents of the organization, especially in their decision-making process. With 43% of reported cases, Corruption represents the second preferred scheme by fraudsters which, in the period between 2018-2019, has caused companies a median loss of $200,000.

To conclude, what is worth mentioning is that contrary to the previous editions which focused their attention just on the United States environment, the 2020 report to the Nation's findings involves all countries. Therefore, the overlapping of the report's results as well as the distribution of frauds among the different categories definitely gives a great evidence of how the phenomenon is globally widespread, but at the same time it highlights how the same schemes still recur throughout the countries, despite the existence of national and cultural differences or barriers. In the next pages the spotlight will be shifted towards the analysis of each of the three fraud categories together with their related sub-categories in order to underline the difficulties and the challenges that companies are forced to face.

1.4 Asset Misappropriation

As mentioned before, Asset Misappropriation comprises all cases in which an individual steals an asset or, more generally, a resource of an organization in order to increase its personal benefit, while taking advantage of the apparent weaknesses of the organization's processes. However, it is common thought that this category goes beyond asset's theft or embezzlement since it also involves the misuse of companies' resources. For instance, an employee using the enterprise's computer beyond working hours, just for its own side business, can't be considered as a theft, but rather it denotes a misappropriation of a company's resource. Since this scheme makes no difference about the company's processes, asset misappropriation can be detected in every small activity of the organization, therefore involving all types of individuals with any form of responsibility, from employees to directors and from clients to suppliers. No distinction is made.

But why is theft considered such a harmful action for the victim company? Very simply, assets in commerce have the purpose to produce income for the organization that makes use of them. In fact, they reflect probable future economic benefits, and this is why they represent the number of resources that a company possesses. However, they can be identified to be part of two different groups, such as tangible or intangible assets, but usually misappropriation concerns the formers, because of their "physically identifiable" nature. Therefore, it stands to reason that, by stealing company's assets the perpetrator is depriving the company from the opportunity of enjoying future economic benefits. For this reason, this type of action represents a potential harm for the victim entity. Going deeper within the fraud tree scheme, which is used as a classification system, it emerges how the Misappropriation category is internally subdivided into *cash* and *non-cash* cases which of course, refers to whether or not cash is the main item stolen during the fraudulent action.

The former category is by far the one which recurs the most, probably because of the nature of cash which can be easily transferred and managed digitally while other resources cannot. In addition, cash is preferable since it can be easily spent without the urgent need to find a specific market to dispose of it, as instead it would happen in the case of other resources, such as inventories for example. However, even if according to the 2020 report to the nations, billing schemes, which belong to cash thefts, are the most common forms of *Asset misappropriation*, non-cash asset's theft follow immediately after them, ranking in second position. Hence, the recurring of non-cash fraud cases is not so uncommon as thought. The reason behind this is probably related to companies' greater concern on the risk of losing cash, such that they normally place stricter controls over cash assets while leaving behind and underestimating controls over non-cash assets. Therefore, by proceeding in order, when analysing the cash misappropriation assets, there are some recurrent sub-schemes which are worth mentioning in order to understand the breadth that this category can have, and also which schemes are recognised to be the most threatening ones from the companies' point of view. Hence, the most common schemes consist of:

- Skimming, that can be defined as a practice through which individuals steal money to the organization before the sale transaction is recorded in the accounting systems. It is important to underline the timing of this strategy since, by removing cash prior to its entry in the accounting systems, no direct audit trial is left. Just to have an idea of how frequent this scheme might be, it is useful to take the 2020 report to the Nation's findings, which summarise the percentage of cases occurred. In relation to the analysis, skimming totalises 230 detected cases with a corresponding median loss of $47,000.
- Cash larceny, which is a practice similar to skimming, but it differs in the fraudulent act's timing, since the theft occurs just once the transaction is recorded on the books and not previously, as instead happens for the skimming. For such reason, the scheme is also known as *on-book* fraud. In fact, in this case the money is stolen from the cash register or directly from the bank's deposits. Evidence shows that Cash larceny accounts just to 8% of the total cases causing $83,000 of median loss.
- Fraudulent disbursement of cash, which is usually pursued by an individual who drives the organization to shell out money in order to acquire a non-existing service or good. Of course, the final aim is to personally benefit from the fictitious acquisition

of the company. The main ways to pursue this practice is by using some specific schemes which can be broken down into:

- Billing schemes: when a company, without realising it, pays for services rather than goods which do not exist, or it also pays more than the actual worth of the service/good. Therefore, the company buys services or goods which are non-existent, overpriced, or even worse, that are not needed. Typically, the company ends up paying for a service or a good even if it is not the actual beneficiary, since the real one is represented by the individual pursuing the scheme. For instance, employees make personal purchases and charge them to their employers by pretending for them to be business expenses.
- Payroll scheme: when a company pays a salary to a non-existing employee or to someone who does not have the right to receive it. For instance, while in the billing scheme the perpetrator usually falsifies invoices, here, in order to benefit from an overcompensation, the employee typically falsifies payroll records and also timekeeping records. The forms through which the scheme is pursued can vary from the application of ghost schemes, falsified wages and also of commission schemes. For instance, 199 cases of payroll fraud schemes have been detected in the 2020 report to the Nations.
- Expense reimbursement scheme: when an employee claims reimbursement of fictitious expenses or rather, claims an amount which is higher than the real worth of the true expenses incurred. For instance, this happens especially when travels and expense budgets are issued as benefits to employees. By falsifying information employees manage to obtain superior compensation of their true expenses. This scheme is ranked as one of the most recurring with 310 reported cases.
- Check tempering: when a company is deprived of money through the emission of checks which are issued in favour of a third party who will be the real benefiter or, also, in favour of the perpetrator's own benefit. As always, the key to pursue such action is to issue false information. In this case the alteration concerns data reported in the check, such that, by submitting it to the victim company, the perpetrator is able to illegally obtain the claimed funds. Hence, it is considered to be a direct form of fraud since the fraudster takes the physical control of the operation. About this, 206 cases of check tempering have been detected within the 2020 report to the Nations.

- Register disbursements: when an individual tries to conceal a fraudulent withdrawal by manipulating the cash accounts. A typical scenario is when a customer returns an item bought from a store and asks for a refund. In this case it should be recorded in the accounting systems that there has been a disbursement of money since the purchase price has been returned to the client. Hence, it could happen that, by recording a fraudulent refund as a legitimate disbursement in the accounts, the employee manages to physically remove the money form the cash register and abscond with it. However, evidence shows that this scheme is the less pursued by fraudsters, accounting for just 3% of all the detected cases.

Other than stealing cash from the company, as previously mentioned, employees can also engage in non-cash schemes in order to personally use the stolen or borrowed assets through improper ways, which could lead to tear and decrease the asset's values. This category can be broken down into two further sub-categories:

- Misuse: which refers to an improper way of using an organization's asset with the aim of using it for other personal purposes.
- Larceny: which denotes a way of subtracting resources from the organization by following some specific schemes:
  - Unconcealed larceny: they are simple thefts of the organization's resources pursued by individuals who are barely interested in using concealing strategies. For instance, there is no attempt to adjust the book accounts in order to conceal the action since the only aim is to walk away with the stolen assets.
  - Assets requisitions and transfers: a way in which an individual asks for the transfer of a specific resource in order to change the place where it is inserted, with the aim of having complete access to it.
  - False sale and shipping: a way in which an individual alters significant documents in order to simulate a sales contract, with a consequent fictitious shipping of the goods in order to conceal a theft happened before.
  - Purchasing and receiving: a procedure by which the goods of a company are stolen during the unloading operation through the alteration of physical documents regarding the shipping and the receiving of the goods.

To conclude, if it is true that specific risks vary based on the nature of the company, this is even more true when considering fraud risks. For instance, financial statement fraud is not considered such a big risk for a sole proprietorship that is not supposed to issue its financial statement to external parties. Equally, for what concerns corruption risk, it is clear to everybody that, in small service-based businesses, it is considered to be very low or even almost non-existent. On the contrary, the risk related to companies' asset's misappropriation, is definitely higher and widespread in all types of organizations since all enterprises have employees and, for this reason, all of them are exposed to the risk of resources deprivation. Not surprisingly, the 2020 report to the Nations highlights how this category accounts for 85% of all fraud cases detected. Therefore, even if Misappropriation of assets does not make front-page headlines as often as financial statement fraud does, it is still the favourite target of occupational fraud offenders. Not to mention how Misappropriation schemes' effects cause an unfair representation of companies' financial statements which instead should be presented in accordance with the GAAP (general accounting principles) system. Therefore, to have a complete overview of this harmful category it is worth identifying three of the major techniques which recur more often in the 2020 report to the nations, such as skimming, fraudulent disbursement, and payroll schemes.

1.4.1 Skimming

With 230 cases reported, skimming is a common fraudulent technique pursued by an individual during a company's selling transaction. The perpetrator's aim is to steal money to the company in an illicit way by acting before the transaction is recorded in the cash accounts. Precisely, because of this specific characteristic, the scheme is also known as *off-book* fraud, or *front-end fraud* which underlines the fact that the theft occurs before the transaction is registered in the accounting systems. Therefore, by taking advantage of the moment before the registration takes place, the individual doesn't leave any sign of its action, which makes it particularly difficult to detect it. In fact, the victim company is usually not aware of the money received from an occurred transaction. What is fundamental to understand about the skimming technique, is that the most important dimension lies on the scheme used to pursue the illicit action and not, as typically happens in fraud cases, on the concealment process. In fact, perpetrator's projected skimming scheme already comprise a good strategy to conceal the action, which definitely makes it a complete process with no further intervention needed. In particular, Skimming can be sub-divided into two further types of categories which are broken down into: unrecorded sales and understated sales. Regarding the former, the strategy is essentially pursued during a sales transaction between a company and its respective client and can usually take place in very busy environments with big spaces for the sales to occur, such as outlets or stores. Here, the most common strategies pursued by employees are represented by cash register manipulations, selling goods even in non-business hours or also through the emission of unregular receipts to clients. Since the fraud scheme is known to be *front-end*, it is pursued every time a sales transaction takes place and each time there is a direct relationship with customers. Therefore, it is worth stating that the opportunity perceived by the fraudster is a consequence of various elements; first of all, of his wide range of independence towards the business operations; secondly, as a consequence of the lack of company's sound controls over the operations and finally, towards the counterpart's incapability of rapidly verifying the outcome. For instance, to clarify the concept, consider a seller of insurance policies working for an insurance organization, who offers a contract to a potential client, submitting him, at a first glance, apparently regular documents. Once the contract is signed, the seller won't record the transaction, leaving the company in the dark and being the only one to benefit from the premiums paid by the costumer, who is totally unaware of the unlawfulness of the contract. This is even more likely to occur if the perpetrator is the only one who interferes with the client in case of an accident, since this would give him the possibility to know the problem in greater advance with respect to the company. This position of advantage would enable him to promptly rearrange the situation in order to keep the scheme uncovered for way longer. However, this is just one of many scenarios that can occur, since the presence of numerous differences in variables such as the company's environment, the number of transactions concluded, the type of relationship established with the client, the cash amount of each transaction and the submission of documents, can modify the fraud scheme in many different ways.

For what concerns the other category which comprises understate sales instead, the procedure is quite similar to the previous one, except for the fact that the commercial transaction is not concealed anymore, but rather it is recorded for a lower amount with respect to its real worth. For instance, during a commercial transaction, it can happen that the seller records a fictitious discount applied to the costumer, with the aim of keeping the amount of the non-existing discount. Alternatively, the seller records a higher amount in the client's document which does not correspond to the one previously reported in the company's accounts. If, on the one hand, the scheme used by fraudsters appears to be very simple and immediate, on the other, it has to face a big problem when relating to the company's inventory system. About this, implementing skimming schemes, as previously said, implies omitting the recording of the commercial transaction even if the latter actually took place. But, by implementing this strategy, there could be huge repercussions on the company's inventory system, since inventories "physically" decrease as a result of the performed transaction. In fact, the items are moved from the enterprise's warehouse. However, on the other side, their book value is kept constant since the perpetrator has not provided for the accounting recording of the related operation. Therefore, this discrepancy between book value and physical quantities represents a first alarm for internal control systems, which should be able to detect that something is not working within the company's procedures. However, even if the discrepancy manages to be detected, it is not easy to really point out the source of the problem since the fraudster's creativity is useful to put into place very effective concealment strategies that manage to circumvent internal controls. Even if the perpetrator's abilities can make it difficult to understand the exact origin of the problem, it is still useful to recognise the presence of an anomaly within the company's systems since it helps to increase the level of attention to be paid to all business's activities and to reduce those opportunities that the perpetrator took advantage of. Therefore, a common way of proceeding is for the fraudster to restrain the frequency of the action and the amount of the stolen value in order to decrease the visibility from the internal controls. At the same time, by doing so, the responsible authorities might believe that, since the missing amount is just a small portion of money, the discrepancy could have simply been the consequence of an error. For this reason, it would worth nothing checking, especially if the detection of the error could require high costs for the company. The previous technique is also known as *Salami technique* since the etymology recalls the idea of cutting a salami in little slices which perfectly represents the fraudster's skill of acting with a restrained frequency and subtracting very small amounts of money each time. This is the reason why many skimming schemes manage to be pursued for many years without being detected and through the years they manage to achieve high economics results.

Another method, which represents a variant of the skimming scheme, is the so-called *credit skimming*, which is likely to happen when a creditor repays the debt towards a company for a rendered service. It seems impossible to commit a fraud in such a scenario, but this actually happens, even if it is considered to be a convoluted practice that requires great abilities and creativity in order for the action to be effectively concealed. For instance, what usually happens, is that a client who has received a service or a good issued by the company is required to pay up the debt, that will be immediately recorded in the company's account in order for the costumer to avoid receiving payment notices and, at the same time, for the company to be able to cash the due amount. It is only when a third party, who is usually someone having access to the enterprise's payment systems, interposes between the customer and the company that the credit skimming takes place. About this, when the client pays the due amount to the company, the fraudster will intervene by directly collecting the amount without recording the transaction on the company's accounts. At a first glance, it could look like as a hazard, but the way in which the third party arranges the situation is brilliant. In fact, the client's due amount, which represents the sum that the fraudster subtracted to the company's accounts, is replaced by a following client's payment and this continues indefinitely since no client receives any payment notice. This technique is known as *lapping* and it costs hard work for the third party, considering that he is constantly engaged in managing the cashflows in order to conceal the theft. However, if the conditions are favourable, the fraudster could also write off the amounts subtracted to the company as bad debt in order to better conceal its actions. The CFAEs found out that skimming schemes generally last 16 months before they manage to be detected, which, if compared to others, it highlights how quick anti-fraud controls are able to uncover them with respect to payroll schemes for example, which typically last 24months. Of course, the quicker the fraud scheme is detected the less damages it would cause to the company.

1.4.2 Fraudulent Disbursement

According to the 2020 report to the nations, Fraudulent disbursement represents just 3% of all the detected cases but still, it is among the six categories which tend to last the most, typically 24 months before being uncovered by internal control systems. The scheme comprises all types of business activities that involve business transactions. A special focus is given to the ones which final aim is to create effective assumptions in order for a company to disburse a certain amount of money in favour of a beneficiary, who of course, is always represented by the fraudster. Therefore, the first apparent difference with respect to the previous strategy is that, while in skimming the fraudster tries to interfere in the relationship between the company and the client directly subtracting the cash inflows, in the fraudulent disbursement the fraudster creates an opportunity, in order to stimulate company's cash outflows and to benefit from them directly or indirectly.

At this point it is worth highlighting how great importance lies on the individual's ability to engage in creative concealment strategies, such as the creation of misleading documents, so similar to reality that they manage to fool the company which will certainly allow for the disbursement. As always, since the fraudster acts only when an opportunity is perceived, it is clear that this type of scheme can be implemented only by employees which have the authority and the independence to approve company's transactions that require cash outflows. Therefore, the role held within the company is an important element which is determinant for the successful outcome of the scheme. However, it is worth stating that there is nothing brilliant in an employee recording a false invoice while retaining the due amount, since this is considered to be an elementary action which doesn't require great abilities. What instead is worth of mention, is the fraudster's ability to circumvent internal control systems while encouraging the company to pay out a certain amount of cash which has not been authorized. For instance, a first method followed by fraudsters to circumvent controls is to sign a collusive contract with a supplier or as an alternative, to create a fictitious supplier through misleading documents, in order to record it as an apparently official company's provider. Regarding the first strategy, it is usually pursued together with another illicit behaviour such as *corruption*, which is used in order to corrupt the employee who works in the fraudster's same enterprise and who has the authority to approve payments, being also responsible of analysing the fairness of supplier's prices. On the other hand, in the second strategy, by creating a fictitious supplier the fraudster has to make sure that the entity is able to operate at least formally, since sometimes the supplier itself is not even registered in the Chamber of commerce as the law requires. However, what matters the most to the fraudster is that the company is able to both submit invoices and cash the amounts paid by the company. For this reason, the fictitious organization is also known as-*shell company*- which recalls the cover role played by the entity, since there is actually no business activity going on. At first glance, by just describing it, this strategy could look easy to pursue, but in reality, it is one the most complicated things for fraudsters to manage because it requires a good premeditation process and a very high threshold of attention. In fact, the most difficult part is the one which requires the individual to fill in the personal data of the entity, together with the location of the registered office and the address to which information should be submitted. All these elements are crucial for the success of the operation, just one error and the game is over. In addition to this, the fraudster should possess a good knowledge of the company's requirements towards the selection of suppliers, such as: what quality standard the company is looking for or also, what prices could attract the company and make the fictitious supplier unique with respect to its competitors. It is important to underline how the difficulty to pursue such scheme changes based on the type of product which is delivered by the fictitious supplier. For instance, in the case of services, it is easier to engage in disbursement, since the product is intangible, and it would be difficult to actually monitor its existence. On the other hand, if the product delivered by the fictitious supplier is instead a tangible good, the situation is even more complicated, since physical products necessarily need a proper space to be kept. To solve this last problem, fraudsters could recur to an additional technique known as *pass-through,* which provides for the involvement of a third entity (real or also fictitious) which is ideally located between the victim company, for which the fraudster works, and the victim company's real supplier. Therefore, the role played by the third entity is to re-invoice the goods sold by the real supplier to the victim company at a higher price, so that the fraudster will benefit from the surcharge, while the company, at a first glance, will have no suspicion when seeing the true existence of the goods. As already stated though, it is important to monitor the size of the surcharge, which should not be set too high, otherwise it would attract the attention of the internal controls and fraud would certainly be detected. However, this type of scheme is not focused only on illicit actions which main purpose is to encourage a company's money disbursement in order to pay its supplier. In fact, some illicit actions are also focused on the mere amount of the payment and on the strategies to pursue in order to increase the correspondent sum. Therefore, these last actions, which are considered to be less complex to pursue with respect to the others, do not provide for the existence of a third party (real or fictitious) which interferes with the victim company and the real supplier, rather they just focus on the employees who possess the authority and the power to collect suppliers' payments. For instance, the so-called *pay-and-return* is a perfect scheme which recalls the above-mentioned actions. There are several ways to pursue this scheme, depending especially on the relationship that the company has with its supplier and the methods of payments and returns required by the latter. However, the most common way is that, once the supplier submits the invoice to the company for which the fraudster works, the latter will proceed by paying a higher amount than it is actually due. At a first look, it could seem a no-sense action, but what the fraudster will do next is to ask the return of the excess payment and once the supplier confirms the return, the fraudster will rapidly intercept the corresponding amount. Similarly, the fraudster, who can take advantage of his position of authority in emitting orders and in controlling payments through the business systems, can push the company to acquire products which the company itself will never benefit from, since the one to actually pocket the money will be the fraudster. To conclude, even if, in general, these actions are not so expensive for the company, they can lead to a sort of emulation of the counterproductive behaviour, to the point that in the long run this could involve more employees to act illegally, with the final consequence of severally damaging the company.

1.4.3 Payroll scheme

Similar to the previous schemes, which main purpose is to benefit from the company's resources by simulating the acquisition of products or services, which however are hardly ever delivered, the payroll scheme focuses on the payroll's manipulation. As is common knowledge, every company has to pay its employees a certain compensation for their work which can be based on the hours worked or, alternatively, on a specific predefined salary. Whether the employees are salaried or hourly, the company is always responsible of keeping time and attendance tracking in order to pay each employee the right amount for their respective work. Since the pay system is composed by many different elements, it can be altered also in many different ways. Two are the recurring techniques. The first one is based on the fraudster's attempt to obtain a higher compensation than the one he is actually entitled to have, and this is made possible by altering for example the number of days off, by increasing the hours of overtime working or by asking refunds for expenses never incurred. Hence, the method pursued is the alteration of physical or electronical documents submitted to the payroll system. The second path instead is the most intriguing one, since it is based on the creation of a fictitious employee also called- *ghost employee*- who is actually registered as an official company worker and who, accordingly, receives the due salary. Not to say that of course, the real beneficiary of the inexistent employee's salary will be the fraudster who is responsible also for the *ghost employee* creation. Therefore, also in this particular scheme the fraudster is able to create a fictitious figure which recalls the *shell company* created in the skimming one.

Even if the logic behind them is similar, there is a huge difference between the two. First of all, creating a ghost employee is a very risky procedure considering that, the probability that human resources can exercises a control over the personnel is certainly greater than controls incurred over suppliers. For instance, many times companies create surveys in order for the personnel to express their satisfaction towards their job or rather they set up training courses to which each worker should participate or interact, thus making it difficult for the fraudster to keep using the ghost employee undisturbed. Secondly, the probabilities of communication with the company's personnel are much higher and especially much more unpredictable than the ones with suppliers. For such reasons, it is clear how occupying an authoritarian position within the company is fundamental for the fraudster's success. In fact, the only way to perfectly control the situation and to face the unexpected events is to be part of the ones in charge of supervising the company's personnel and to manage all the related practices. Considering all these elements, it is not so trivial to perfectly coordinate each aspect without being detected and this is why this scheme is generally pursued within organizations that have very poor internal control systems or where one or more employees, belonging to the highest levels of the hierarchy, enter in collusion. Evidence of this can be found in an ACFE report named "Ghost do exist", based on a case-study, where a woman embezzled more than $100,000 from a non-profit organization for which it worked, just by creating ghost employees. How could all this pass undetected? The report stated that: "*Her scheme went undetected for three and a half years because the company lacked sufficient controls to prevent and detect this type of fraud. Specifically, no other employee was involved in the payroll process; the fraudster had sole authority for adding and removing employees from the payroll and for running and distributing pay checks each pay period. Additionally, the company did not have a reporting mechanism for other employees to report suspicious activities or an internal audit department to review the operations and finances for signs something was amiss. The employee never took vacation, and she came into work sick rather than take time off*". This example enables to point out how such schemes are completely indifferent to the type of organization since they can also occur in non-profit organizations as the above-mentioned case shows. In addition, it underlines how the lack of sufficient controls and also the role covered within the organization represent great opportunities for the fraudster to act undisturbed.

As an alternative to the *ghost figure*, which requires a great level of attention in the registration of coherent personal data and other personal information, the fraudster could also take advantage of employees leaving the organization. In fact, when an employee leaves the enterprise one of the first steps is to ensure that his access to payroll or HR systems is definitely removed. But of course, if the fraudster takes control of this process, he would be able to distort the procedure by keeping the employees' access to the systems still active. By doing so the fraudster's responsibility would consists just of using the valid pay-roll record of ex-employees which would make it way simpler to pursue with respect to the creation of a completely new figure. Despite the simplicity of using ex-employees accounts, the ghost scheme is one of the most surprising strategies used by perpetrators since it enables to generate new fictitious identities within organizations that are constituted by many concretely working employees. By analysing the situation externally, it looks quite a hazard, something impossible to pursue, especially if considering that within enterprises people have daily relationships. Moreover, employers look out for employees' results and each of them is associated to a particular function within the company. Therefore, it is quite easy to realize if a colleague is present or rather, he is missing since employees work in a relatively closed area. For such reasons, instinctively this path appears to be unfeasible. However, by looking at it from a different perspective, this situation appears to be more viable than it seems. For instance, nobody really knows how many employees are registered in the company's payroll system and what's more, nobody really knows who is responsible of verifying the perfect match between the registered employees and the effective number of those working within the organization. Therefore, it is clear how the fraudster could take advantage of the previous aspects in order to pursue the scheme. This means that the will to commit crime can be detected everywhere even where ordinary people could find it illogic or impossible to pursue. Out of all aspects, payroll is an important process for the employee's morale since through this processing employees perceive their net worth within the company. Therefore, if at any point in time payroll is late, employees could question this delay which in the long run could give origin to the already mentioned "undue pressure" within Cressey's fraud triangle theory. At the same time though, such frauds happen for many other reasons besides the payroll timing, with the most common one being employees' sense of greed. Overall, by analysing the potential impact that the different fraud categories have over organizations, the 2020 report to the Nations highlighted how the payroll scheme occurred in 9% of all detected cases, causing a median loss of $62,000. Even if it is not ranked as one of the most harmful in economic terms, it is still recognised as the one lasting the most, together with *check and payment tempering, register disbursement, financial statement fraud, expense reimbursement and billing schemes*. In fact, the report shows that anti-fraud controls typically take 24 months before uncovering these particular schemes.

1.5 Corruption

Practiced all over the world, Corruption, is now a well-known phenomenon that, according to the 2020 report to the Nations, has caused companies, in the period between January 2018 and September 2019, a median loss of $11,100 per month. It has also been ranked as the second scheme, just below financial statement fraud, which is able to cause the highest damages in terms of velocity. However, even if these data should be used to prioritize company's investments in mechanisms to prevent such scheme, evidence in the report shows that company's anti-fraud systems still need 18 months before uncovering this type of fraud, probably because the victim company results attacked from two different directions at the same time. In the fraud tree, corruption is divided into four particular sub-categories: bribery, economic extorsion, illegal gratuities and conflicts of interests. Among the four there are both similarities and differences which are worth mentioning in order to have a complete overview of the phenomenon.

For what concerns bribery, it is defined as *the offering, giving, receiving, or soliciting anything of value to influence an official act* [8]. However, bribery can also occur within commercial transactions when something of value is given in order to influence a business decision. Regarding this, it is important to highlight that payments are part of companies' everyday life since they are used to influence business decisions. For instance, the subscription of a contract between a buyer and a seller occurs because something of value is offered. Therefore, these types of payments are totally legal since they are perfectly in line with everyday business. However, when bribery occurs, payments made to employees are not considered to be legal since what is missing is the employer's authorization. Hence, bribery involves *under-the-table* payments in return for the exercise of influence over a commercial transaction. For what concerns gratuities, these schemes appear to be similar to bribery with the exception that something of value is given to an employee in order to reward him for a decision and not for having influenced the decisional process. Of course, the decision for which the employee is rewarded provides benefits to a specific company or alternatively to a specific person. To clarify the concept, if an employee working for a utility company manages to award a construction contract to a certain company, he will be rewarded later on with something of value, such as a car for example. Even if, at a first glance, receiving such gifts seems harmless, some companies have recognised how this scheme could easily evolve into bribery and, for such reason, they have introduced strict ethical policies in order to avoid the acceptancy of unreported gifts from clients. In fact, one of the consequences of gratuities is the risk that the involved employee reaches an agreement with the same supplier for future transactions or alternatively, that he directs the contract to a certain company with the hope that later on he will be rewarded with a gift. Finally, the last scheme is represented by extortion, which is also identified as "pay-up-or-else". Here, instead of paying to influence

[8] Association of Certified Fraud Examiners, *Fraud Examiners' Manual*, Austin, TX:Author, 2011

a business decision a person asks a payment from another. In case of a refusal to pay the extorter, this could result in a loss of a business. For instance, an employee could demand a payment from a supplier in order to award him in return a subcontract on a specific project.

What is corruption then, and how can the term be defined? Corruption is considered as a form of dishonesty, that usually arises when an individual offers, gives or receives something of value in order to influence a third party to act against its duties, or rights of others, thus acting illegally. Many have been the intentions and the efforts to eradicate the phenomenon from society but still, corruption, has managed to resist and to evolve in response to the changes of the social, economic, and cultural context. However, there are still long debates regarding the definition of the phenomenon. It appears very difficult to find a common and shared delineation of the term, due to the existing difference in countries' legal approach, as well as in the sensitivity perceived towards the phenomenon. What, instead, meets the general approval is first of all, the idea that the phenomenon is not something apart or an isolated event. In fact, the latter can be compared to a spiral that starts with a corruptor becoming a corrupter, as a form of debt repayment, and indefinitely continues with the corrupter becoming a corruptor, with the aim of obtaining the desired benefit through the illicit acquisition. Secondly, it is clearly a phenomenon which occurs in a private and reserved way through power abuse, and which generally requires a stable relationship between two individuals, identified as the delegator and the delegate, in order for the former to acquire illicit benefits through the second one. However, such benefits are not always necessarily economic benefits, it depends. An additional feature of corruption concerns the typology of the act, that changes in relation to three particular elements, such as the relationship established between the corruptor and the corrupter, which is fundamental to determine whether it is a continuous relation or just an occasional one; the benefits that the corruptor aims to obtain and finally the result that the corrupter wants to achieve. Therefore, depending on the variation of these elements the typology of the illicit act will accordingly change. Interestingly, when surfing the internet to acquire additional information about corruption, the first thing mentioned is that the phenomenon occurs mainly in the public sector, eroding people's trust in it. However, it is worth adding that it is not just something which exclusively belongs to the public sector rather, it affects also the private one, which will be object of further analysis, since the focus of the chapter is fraud pursued within organizations. What is also important to keep in mind is that organizations are not always victims of corruption, but they can also be the actors of such illicit actions, especially when involved in commercial transactions with other companies. For instance, a company willing to obtain a contract in order to be the official supplier of a certain client enterprise, could indulge in corruption by offering any kind of reward to a client company's employee. The latter should be covering a high level in the hierarchy, such as being the responsible for the purchasing process, in order for him to influence the company's decision towards the acceptance of the proposed contract. If on the one hand, many evaluate this action as a mere illicit behaviour that does not harm any public interest, on the other hand, many believe that this action, in the past, has produced great damages up to the point that it has undermined investor's trust in the company, causing harmful financial repercussions. Therefore, even if it is simple and more immediate to see, the attention should not be addressed just towards the type of "reward" offered to the subject of the client company, but rather on the distortion of the company's operating processes, which are anything than correct, transparent, and regular. This of course, is symptom of other unfair procedures pursued within the organization which represent fertile ground for corruption to flourish. In addition, assuming that the corrupted subject manages to convince the company to accept the supply contract, it is interesting to notice that, in order for the corrupting company to reward the subject, it has to engage in several other illicit actions, for instance asset misappropriation, which represents a concealed procedure. In fact, going back to the previous example, what is important to highlight is that the damage caused to the organization is the distortion of the selective process used to choose the most convenient supplier, since the only and exclusive aim is to increase the economic interests of third parties, rather than satisfying the supplier's company goals. Therefore, the corrupting company, who manages to be selected as the official supplier, is able to freely set high prices in order to use the margins, which derive from its product selling, to repay the unfaithful individual, who is part of the victimized company. However, as previously stated, the scheme changes when certain conditions also change and what can happen is that corruption towards a member of the client company could have as a final aim the signing of a tacit contract of exclusivity, without the imposition of any other kind of condition in relation to product prices, rather than to their quality or quantity. Even if this, at a first glance, may result as less harmful than the previous case, where the corrupter pushed to increase the purchase price, here the client company is still condemned. In fact, in the long run this exclusive relationship could lead to boost the supplier's confidence, up to the point that it will have no more stimulus to respect the market competitive conditions.

Whatever the scheme is, evidence shows that corruption is a predetermined, intentional, and concealed action which aim is to induce, through a reward, a corrupted individual to act improperly in its work functions in order to obtain a benefit. About this, it is quite easy to mix up terms such as "corruption" and "conflict of interests", which most of the times are wrongly used as interchangeable. When considering the fraud tree within the 2020 Report to the Nation, it is clear how "conflict of interest" is just a subcategory of "corruption", which means that they are actually not the same thing. In fact, by lingering on the concept of "conflict of interests" it emerges how this term simply recalls the existence of a situation where a subject who has, within the company, the professional responsibility to decide or act for the benefit of a third part, such as company's clients or stakeholders, is simultaneously involved in personal interests. This double interest could lead the individual to act with a sort of inefficiency especially in the fulfilment of its duties. Here is the turning point. When referring to *conflicts of interests* the focus lies on the risk of a possible interference while, when talking about corruption the focus shifts on the possible risk of power abuse. Clearly, the two concepts are completely different. For instance, a subject which is involved in a "conflict of interest" may never end up indulging in a corruptive action, which, accordingly, represents just the last step of the process, when unfortunately, the situation degenerates. This is just to highlight that "conflicts of interest" do not necessarily lead to corruption, rather their presence could represent a potential risk for the organization, especially when the interest is left undisclosed. Other particular fraud schemes take place also during tenders, private or public indifferently, which represent the perfect scenario for corruption to flourish, since different companies are involved in a competition aimed at obtaining a specific supply contract. Any company which is able to take advantage of its competitors by illegally exercising its influence can benefit from it, winning the tender.

To have an overview of the importance of the phenomenon, in a report published by ANAC[9] (Autorità Nazionale Anticorruzione) that considered the period between August 2016 August 2019, 28 episodes of corruption were recorded respectively in Sicily, 22 in Lazio, 20 in Campania, 16 in Puglia and 14 in Calabria. What is interesting about these numbers is that 74% of these episodes were related to the corruption during public tenders, which confirms the relevance that this sector has in relation also to the illicit interests that arise due to the high economic volume involved. In the same report, the president Raffaele Cantone explains how the methods of bribery payment, which take place in order to win the tender, have

[9] Autorità Nazionale Anticorruzione, *La corruzione in Italia (2016-2019) numeri, luoghi e contropartite del malaffare*.

literary changed during these years and that a new form of bribery dematerialization is becoming more and more popular. In fact, if on the one hand, greed is what motivates people to be rewarded through cash, on the other hand, the implementation of controlling systems and the increasing difficulty to justify the proceeds, has led people to change the nature of promised rewards. At the first place, still based on ANAC's latest report, corrupted people ask for a job position, followed by professional services, especially consultancy. However, if these are the most common ones that occupy the highest positions in the ranking, it is worth also mentioning the new ones which are catching on, even if recently introduced. Such rewards range from different types of benefits (gasoline, food stamps, travels) to building renovations and from the offering of cleaning services to furniture transportation. The corruption scheme reported on the ACFE's report examines the phenomenon through the victimized company's prospective, posing the focus on its corrupted employees and on their respective actions, which inevitably go to the company's detriment. It highlights how, since corruption is a dishonest action which is able to harm the company and erode its corporate values, directors, of any sector, are always very concerned about the spread of this phenomenon and on the possibility that it could cross the threshold of their respective companies. For this reason, great attention is paid to each of the company's processes, especially the ones involving purchasing practices and supply contract's evaluation, in order to be sure that there is no longer any opportunity for employees, especially for those covering the role of purchasing manager, to indulge in dishonest actions.

1.6 Financial statement fraud

Contrary to what is common thought, companies' balance sheets are not part of a useless fulfilment required by law, but rather they represent the mean through which companies communicate their actual health status to all users, such as suppliers, investors, and banks in order to obtain the essential support. In fact, financial statements represent companies' financial and economic conditions through the reporting of four main documents: the balance sheet which reports all the assets, the liabilities and the owner's equity; the income statement which reports the revenues and the expenses incurred; the cashflow statement which represents the sources and the uses of cash by the company and finally a section which is exclusively reserved to the reporting of all information that specify the methods of accounting applied, their changes, the contingencies and so forth. As a complemental tool, there is also the option to insert a management report, known as Management's discussion and analysis, where executives can report their perspective regarding the achieved results. Therefore, what does financial statement fraud provides for?

The scheme focuses on premeditated actions, which provide for the deliberate manipulation of company's accounts, in order to mislead financial statement users, who have economic interests in the company and who base their decisions on the company's financial conditions. The aim of this action is to show an organization's apparent solid financial position, in order to convince stakeholders such as creditors, investors, and lenders, that the company is a well-managed entity and deserves confidence. Therefore, the primary aim is to not lose trust from stakeholders, where in Italy the majority are represented by banks. Since the manipulation procedure involves specific characteristics, it is clear how it can be pursued only by personnel who possesses a high level of authority, combined with high skills on the related topic, such as the upper management team. Evidence of this is reported in the 2008 Report to the Nation, where the majority of the detected cases, respectively 53,3%, were pursued by the owners/executive's category, which coincidentally also represented the category with the highest percentage among all the other types of schemes. In fact, regarding the reported asset misappropriation and corruption cases, owners and executives were responsible just for the 22,2% and 37,3% respectively. The latest report, however, highlights also other interesting aspects of such scheme. About this, financial statement fraud has been ranked as the first scheme to be the quickest in harming the company, with a corresponding median loss of $39,800. Additionally, in order to uncover it, the company usually takes 24 months, which definitely makes financial statement fraud one of the most long-lasting schemes. Such results should help the company to understand where to direct their respective anti-fraud efforts, since not all schemes affect the company in the same way. However, it is interesting to consider how just 10% of the 2020 report's detected cases, concerned financial statement fraud, while instead, the median loss caused by the latter amounts to $954,000. A huge number compared with the one caused by the other types of fraud. There are several ways in which fraud can develop within financial statements and these go beyond the misapplication of accounting principles. For instance, it is common practice to draw up false documents, indulge in their alteration or also in the alteration of accounts and transactions. Giving an untrue representation or even worse, omitting to report transactions or events is a second way of pursuing the scheme. Moreover, the reporting of incorrect information, which should be used as a complemental tool to the financial statement, or in addition, the application of aggressive accounting techniques during the financial statement preparation, which takes advantage of the flexibility existing within the regulatory framework, are still considered forms of fraud. Since the methods can be many and diversified, the chapter considers just some of these schemes, in order to point out the most commons ones, which still represent a good way to understand the phenomenon.

Before entering into the strategies, it is worth stating how accounting, which is the tool through which the scheme is undertook, has significantly evolved during the years, in relation to the changes of the economy throughout the world and also to the changes in what are the user's evaluating logics of such information. These changes resulted in a modification of the balance sheet structure, together with the nature of the reported values, such that now the spotlight has shifted towards intangible assets/resources. These are the product of accurate estimating processes. At the same time though, this progressive change has assigned major weight to summary values such as EBIT for example, which denotes the cash flow produced by the company's core activities, and also to qualitative information, such as segment reporting that engraves on the different fraud schemes. A second aspect to highlight, is the importance to have a correct approach towards the definition of financial statement fraud. In fact, it is common thought that this expression encloses only some specific cases, but this incorrect perception could lead to the underestimation of other important and more insidious ones. In fact, when relying just on the pure dimension of "accounting" it is easy to get mislead. Doing so would imply that only behaviours which recur to the manipulation or rather to the alteration of accounting rules, with the aim of giving a distorted representation of the company's performance, are considered to be proper of fraud. For instance, recalling to the above-mentioned scenario, the advanced recording of sales receipts or the capitalization of expenses, which should rather be recorded in the income statement, are typical examples of fraud, since they both correspond to violations of the accounting principles. However, by posing the above assumption then, it is automatically true that, if fraud is related just to the violation of the accounting principles, then every other behaviour that correctly applies the accounting principles, would instead lead to the truthful representation of the company's financial condition. This is not the case though since financial statement fraud is much broader than this prospective shows. What is missing in the prospective, are all those situations in which operations are realized as an instrumental way, just to pursue an illicit act. For instance, if a manager who is responsible of preparing the financial statement and who possesses a strong knowledge on the accounting principles, architects one or more correlated operations just to conceal some values, while however giving a truthful representation of these events, it is still to be considered fraud. In fact, the object of representation would be the "form" and not the effective "substance" of the operation.

A clear example of this is given by the so-called *back-to-back operation*, which in origin, before derivatives were introduced in the financial system, was firstly used as a method to mitigate the exchange rate fluctuation. Subsequently, on the basis of its specific characteristics, the back-to-back was used as fiduciary contract with collateral as a guarantee. This last feature made it a great instrument in order to transfer funds towards occult beneficiaries, especially within the banking sector. About this, the fraudster, usually the CEO of a credit institution, orders for a fund's transfer towards one or more of its checking accounts, opened in other banks which represent the intermediate entities. At this point, the CEO, through specific instructions, asks the highest exponents of the intermediate banks to provide a contextual loan of the same amount to an entity or a subject related to him, which is usually the final beneficiary of the operation. The disbursement of the loan is done without any real or personal warranty, and it is also provided in the long-term, since what acts as a collateral to the loan, that is granted to the final beneficiary instead, is the initial deposit made by the credit institution towards the intermediate banks. Therefore, by analysing this operation it is clear how this operation is aimed at obtaining two main benefits: the concealment of the theft of company's resources in the balance sheet, by representing something different than reality, and the ability to protect the flows of the stolen assets, which are used for illicit actions, from the attention of competent authorities. The initial fund, transferred by the credit institution towards the intermediate banks, is represented in the current asset section of the corresponding balance sheet instead of being reported in the fixed assets one. This scheme truly occurred in 1981 with the credit institution of Banco Ambrosiano Italia being the corresponding perpetrator. The latter has been accused and detected while transferring large amounts of money to its deposits in an intermediate bank which, in turn, has been responsible for delivering the corresponding amount, under the form of a loan, to other foreign banks. Clearly, all this has been concealed through a perfect representation of the balance sheet accounts, such that Banco Ambrosiano recorded all the deposits in the current assets section, instead of recording them as loans in the fixed assets. Therefore, all transactions are perfectly licit, but what instead has illicit characteristics, is the correlation between the transactions and the aim pursued. The whole of the two, have the power to make the account's recordings result as untruthful. The above-mentioned scheme is the starting point to understand how to approach the financial statement fraud, since the right emphasis should be given to the substance of operations rather than to the form, which means that primary importance should be given to the "truthfulness" aspect. As the ACFE highlights in the 2020 report to the Nations, financial statement fraud can be subdivided into five main categories which very briefly are:

- Fictitious revenues, which imply the recording of non-existing revenues in the balance sheet.
- Timing differences which refer to the misapplying of the competence principle or, in the case of revenues, to the misapplying of the rules relating to their recognition.
- Improper asset evaluation which refers to the underestimation or also overestimation of books values due to an improper use of the estimation methods.
- Concealed liabilities and expenses which relates to the exclusion of certain operating costs.
- Improper disclosure which relates to the disclosure of insufficient qualitative and quantitative information which is specifically required by law.

1.6.1 Fictitious revenues

Fictitious revenue's scheme primary aim is to boost company's revenues, by recording transactions that never occurred or, rather, that were realised for smaller volumes. Therefore, it is a process that deliberately adds revenue that does not belong to the company. But before going deeper into the concept it is important to state that there is a specific accounting principle to follow in order to properly recognise revenue. About this in fact, revenue has to be recognised when it is realised, or it is realisable and earned. The financial accounting standard board (FASB) codified "revenue recognition" in order to provide a guidance on the revenue recognition criteria to follow. Hence, revenue is considered to be realisable when four circumstances are contemporary met. The first requirement is for persuasive evidence of an arrangement to exist. Secondly, revenue is realisable only if the delivery has occurred, or services have been rendered. Third, the seller's price to the buyer is fixed or determinable and finally, collectability is reasonably assured. Therefore, a perpetrator willing to boost revenues will certainly misapply these four criteria. But why should someone within the company try to increase revenues? There are several reasons behind it, but the most recurrent one, is that many times directors aim at reaching their sales targets in order to receive a promotion, or rather, a bonus for the goal achievement. In fact, departmental budget requirements can sometimes lead to financial statement fraud occurrence. The ways in which this scheme can take place is through the involvement of fake customers or rather through the stemming of real existing customers. Regardless of the scheme used, in order for it to be successful, it always requires the preparation of documents which final aim is to simulate the real occurrence of transactions. Of course, in the case of goods sold, the creation of such documents is definitely more complicated since material products are known to be tangible goods with respect to services which are classified as intangible. However, when the fictitious transaction takes place and the company records the respective credit on the accounts, a huge problem arises, since this credit is meant to be non-performed for an indefinite amount of time. Of course, by not managing this problem the fraudster could run into the risk that, the respective lack of cash inflow, could make internal controls suspicious up to the point that fraud could be easily detected. To avoid being uncovered, it is important to use effective credit concealment strategies, which are the result of a combination of both fraudster's creativity and opportunities. About this, two sub-categories can be identified: the first one relies on a third party's collusion in order to conceal fraud, while the second one relies just on technical-accounting skills solutions. Despite its apparent simplicity, the former is the most complex and sophisticated one to be pursued. In fact, the strategy requires an efficient coordination of the third party involved. It also requires the ideation of a solution in order to provide the latter with the necessary resources to pay off the credit generated from the recorded fictitious transaction.

A typical sophisticated scenario can be characterised by the presence of three entities, such that A is the company willing to illegally boost its revenues, B is the independent company which usually interacts with A through commercial transactions and finally C, which is related to B trough participative constraints. The latter will also be the final entity responsible of A's credit repayment. Therefore, what is the utility of involving two different types of entities, respectively B and C, in this scheme? Well, C is the company which receives the fictitious sale and that is responsible of paying its due debt, thus generating A's cash inflow, which is the necessary element for the company to keep the scheme uncovered. Company B, on the other hand, is the mean through which A transfers the sum corresponding to the owed credit to company C, in order for the latter to repay the fictitious shipping. At the end of these operations company A will manage to finally record a positive variation of cash, which corresponds to the amount received by C and that will successfully validate the fictitious transaction. Such scheme, that can be pursued in many other ways just by modifying one the previous features, is the most complex one to be implemented, since it requires the involvement of many different subjects (or entities) as well as the involvement of a great number of transactions, regardless of whether they are fictitious or real ones. In addition, the scheme has to deal also with different timings for what concerns the payment and the billing activities. Another variant of the scheme is the one pursued by Parmalat company, the Italian entity, known all over the world for the fraudulent bankruptcy occurred in 2004, which pretended to sell 300.000 tons of powdered milk to its Cuban customers. The total value of the fictitious operation corresponded to $620 million, which permitted the company to boost its sales and consequently its revenues. The operation consisted in the double invoicing scheme, which permitted the company to recorded two invoices, a real one and a fake one, in Parmalat’s accounts, while issuing just one invoice to the Cuban customers. Therefore, in this scenario the customer figure really existed, what instead was made up was the great number of powdered milk tons recorded by the company on its balances sheet. The second sub-category of financial statement fraud instead, detaches from the practices of collusion with third parties and relies just on sophisticated accounting adjustments in order to pursue the same aim: set to zero the non-existing credit. For instance, if the amount of money to be concealed is just marginal, a company can easily pretend to be involved in a sales transaction and can easily pursue a sales adjustment, together with the corresponding credits adjustments and record a return on sales, for an adequate value, just in a second moment. It is particularly interesting to notice how this scheme, contrary to the one relying on collusive agreements, doesn’t provide for any cash inflow or outflow, but rather it involves just mere accounting practices. In conclusion, this type of fraud category can involve very harmful schemes which firmly rely on non-existing transactions in order to boost company’s revenues. The different types of schemes pursued can impact differently on the perpetrator’s balance sheet structure, since many of them can indirectly modify the operating income. For instance, recognising fictitious costs as extraordinary components, which however are not to be registered within the company’s core activities. Other schemes instead, leave the structure as it is by balancing it through the recording of both fictitious costs and revenues.

1.6.2 Timing differences

IAS 18 (paragraph a) states that: “*Revenue from the sale of goods should be recognised when the entity has transferred to the buyer the significant risks and rewards of ownership of the goods*”. Since Fraud is known to act outside the regulatory framework, the most common method used in order to circumvent IAS 18 is for companies to illegally recognise revenue earlier. Similarly happens with expenses and liabilities which follow the same logic of revenue recognition, with the only difference that they are illegally recorded later on, in order to mislead the financial statement and boost the net income. Therefore, since the underlying logic is similar for the two, the chapter will focus only on revenue recognition. As the word recalls, timing differences is a scheme which aims at purposefully altering the financial statement by anticipating or delaying the transaction's recordings, such that this practice strongly influences the business profitability result. What usually happens is that companies keep the books opened past the end of the accounting period, in order to record higher revenues. This practice is also called *cut-off*. At a first glance, this playing with time could appear as a mere attempt to simply alter the recognition moment of a value, instead of altering the actual existence of it. Hence, it could appear to cause less damage to the truthfulness of the company's balance sheet. This is not the case though, considering that for example, the early recognition of a revenue could be the outcome of a fictitious transaction or rather of a transaction which has not been concluded due to the related third party's non-compliance with the contract's terms. It stands to reason that, in the case of a fictitious transaction or also, of a third party's non-compliance to the terms, the scheme will result in the early recognition of a non-existing revenue. Therefore, this strategy should not be underestimated, since it can seriously damage the company with the same intensity as the other schemes, or even worse, since it is quite difficult to detect it. It is worth analysing the different forms in which this scheme can be articulated in order to have a broad overview of its development.

A typical situation is represented by the existence of non-contractual agreements which are, for obvious reasons, concealed with respect to the ones proper of the transaction. In fact, these non-contractual agreements, also known as *side-agreements*, are independent agreements which are used within a transaction to modify the real nature of the operation or also to modify the terms of a sales contract. Therefore, by stipulating *side-agreements* the party involved in the sales transaction can establish, for example, personal terms regarding the rights for returning a specific product or also the possibility to cancel the operation when prompted, with the final result of totally influencing the accounting of such values. Similarly happens in the *channel stuffing* scheme, which final aim is still to boost revenues, but in a slightly different way since the company tries to ship more products to distributors and retailers even if these exceed their actual needs, thus leading to a condition of overbuy. This happens particularly within industries that are known to have very high gross margins since this could help them to increase short-term sales. For instance, pharmaceutical industries, perfume industries or also cigarette industries are the ones mostly involved with the channel stuffing strategy. Such scheme is usually complemented by the above-mentioned *side-agreements* that enable the distributor, or the relative retailer, to obtain discounts, extended payment terms, rather than the possibility to return the products in excess to the issuer company at any time. It is clear how this procedure enables the company to increase its sales figure just for a temporary period and to show its capability to achieve the earnings targets. The early recognition of such revenues, however, will certainly lead to a following and infinite adjustment of the book values. In fact, distributors, who were forced to purchase products in excess, will not be able to sell them all and will accordingly send them back to the issuer company, thus complicating the accounting records.

Many are the examples reported on the newspaper headings which relate to the use of timing difference schemes. For instance, Midisoft corp. in 1994 declared that it diligently complied with the accounting principles by recording revenues just once the product shipping was made. However, this was not what actually happened within the company since managers, responsible of the financial statement preparation, were found to record revenues even if products were not yet shipped within the respective financial year. Of course, the problem of leaving books opened past the end of the accounting period, is related to the fact that there is no reasonable assurance that the counterpart will actually pay for the delivery, thus creating big problems if the situation diverts from the company's expectation. Not to mention that this illegal practice misleads the whole financial statement representation which clearly goes to the user's detriment. Additional elements which represent big issues for revenue recognition are long-term contracts. In particular, construction contracts can be arranged using the *completed contract method* or alternatively, the *percentage of completion method*. While in the former the revenue is not recognised until the project is 100% completed, in the second one revenue and also expenses are recognised as measurable progress on a project. Therefore, the percentage of completion method is more likely to be manipulated since managers can easily modify the percentage of completion and the costs estimation with the aim of recognising revenue prematurely. Therefore, what motivates directors rather than CEOs to manipulate the accounting values by reporting them in improper periods, is the consequence of different contingent elements, such as the achievement of a predetermined sale volumes and the achievement of a target profit, especially if the result is rewarded with personal bonuses. Other reasons concern the desire to keep the competitive position gained within the market, in order to keep up the company's stock, or also to show a high profitability when the company is involved in a business transfer. Considering the above-mentioned reasons, it is important to keep in mind that perpetrators are not concerned about the effects that the manipulation of the accounts could have in the long run, since their aim is to operate in the short-term to achieve immediate benefits. It stands to reason that, mentioning this is extremely important in order to understand the logic behind fraudster's actions since sometimes they could appear to act illogically, especially to people who usually comply with the accounting principles, in this case with IAS 18. Being unaware of perpetrator's way of thinking could lead auditors to underestimate some important situations, with the result of leaving fraud schemes uncovered.

1.6.3 Improper asset valuations

As the world economic system has undergone through an evolutionary process during the last centuries, company's assets have consequently changed both their composition and the combination of the elements that contribute to their formation. In fact, when considering production processes, forms of investment and different forms of financing it is clear how each of them has turned to be a very sophisticated procedure, which most of the times is influenced by elements that lack the physicality requirement. This particular feature has complicated the procedures regarding data collection, data processing and data synthesis which have also been undermined by the particular attention paid to accounting values obtained through estimating methods, rather than directly obtained through commercial transactions. At this point it is important to highlight why these estimating methods are so crucial in this particular section. About this, it is well established that accounting principles set out the guidelines in order for companies to correctly comply to the norms, but what is also true is that the ways in which the accounting principles are applied, commonly depend on the actual context that the company is having to face or, rather, on its management team's opinion. This sort of flexibility on the compliance with accounting principles can lead to manager's engagement in aggressive accounting practices. By doing so, managers can take advantage of certain estimation criteria in order to express their optimistic projections and, at the same time, exercise a sort of discretion when reporting numbers. For instance, managers could use aggressive accounting practices to report generous levels of bad debt in the financial statement, such that the resulting provision would exclusively depend on management team's credit recovery judgement. This of course works as long as estimations are reasonably justified. Therefore, it is clear how the border line between aggressive accounting practices and fraud can be very thin. In fact, it is complicated to understand where aggressive accounting ends and fraud instead begins, since managers can mislead the financial statement representation by abusing of intrinsic subjectivity.

The elements on which the fraudster usually concentrates its attention are the closing inventories, credits, bad debts, material/immaterial assets and all the other items involved in subjective measurements, since their values can be easily manipulated. While analysing closing inventories, for example, it is clear how, contrary to sales, purchases or personnel costs, this category is more exposed to the attribution of incorrect values. About this, the accounting principles (of the Italian Civil Code) require that the value of closing inventories should be written at the lower between their cost and the market value. However, since ending inventory's value cannot be read in external documents, as instead happens for purchasing invoices, in order to determine their actual value, it is necessary to take stock of what is left in the warehouse and compute the remaining units. Subsequently, it is necessary to identify the value to allocate to the computed units. Of course, in the case in which the closing inventories refer to semi-finished or finished products the situation becomes more complex, since many times companies are not even able to correctly determine their respective production cost. In addition, by looking at it from an external view, and just by relying on public information, it is quite impossible to get to know how many units of inventory are left in a company's warehouse or even to know how many of them the organization will be able to sell, at least at a price that equals their corresponding cost. For this reason, it is immediate to understand how companies facing difficulties or worse, losses, could take advantage of this situation to manipulate the balance sheet by increasing the closing inventory's value, which will consequently increase the results for the year. It is important to add that by applying this illegal technique, companies could be severely affected by the so-called *boomerang effect*, which refers to the fact that by increasing inventory's values the company will surely have to deal with higher costs in the next period.

Other common schemes that can impact on the balance sheet assets concern the capitalisation of items, which, however, do not possess the required features to be capitalised; the purposefully use of the fair value to determine the acquisition cost, rather than relying on the historical cost and vice versa. A typical scenario is represented by the lengthen of asset's depreciation life. About this, it is established that depreciation is a process which does not generate cash outflows, but rather it is used to attribute a part of an asset's historical cost to each period of its life, such that each depreciation charge is reported in the income statement section. Of course, in order to determine the asset's useful life, it is fundamental to estimate for how long it will be able to generate revenues to the company that employs it in its productive process. Therefore, managers whose final aim is to reduce the impact that expenses have on the financial statement, in order to make the company result more appealing to investors, will certainly change the asset's life by lengthening it. Hence, by increasing the asset's life, the depreciation level, which is respectively recorded in the income statement since it represents an expense, will accordingly decrease. Undoubtedly, this practice is totally legal if the assumptions made by the management team on the asset's life can be reasonably justified, such that there is a real belief that the asset lasts longer than it was previously stated. Otherwise, if the purpose is just to increase profits, then it will surely result in a fraud scheme.

1.6.4 Concealed liabilities and expenses

If in the previous chapters the focus was set on sales and fictitious revenue increases, in this specific category the spotlight shifts towards expenses and liabilities concealment. The technique is also known as *off-balance sheet financing* and many companies generally indulge in it when they want to record their assets but not their liabilities. Clearly, the main reason here is still the same as the previous schemes: to show a stronger picture of the balance sheet. However, the fraudulent scheme could also be used to avoid a hypothetical loan covenants breach, such that by showing too much debt the company could be exposed to a dangerous situation. The ways in which the scheme can be pursued varies depending on the company's specific context. For instance, just to introduce a well-known scam happened in 2001, Enron, the USA energy company, possessed many unconsolidated subsidiaries. The possession of unconsolidated subsidiaries meant that all subsidiaries' expenses and liabilities were not meant to be reported on Enron's consolidated balance sheet. By doing so, subsidiaries could be easily used as secret funders of Enron's operations, since the money raised by those entities stayed off Enron's books. Of course, this allowed Enron to show a stronger picture of the company and consequently to maintain a higher credit rating that otherwise it would not have deserved. Not even the time to digest the scam that only a year later another accounting fraud came in light, but this time WorldCom, the US telecommunication company funded by CEO Bernard Ebbers, was responsible for it. The pursued scheme, however, was totally different from the previous one, but still, the main objective was to decrease expenses in order to be more appealing for investors. In this case, the company had been accused to capitalise expenses which instead should have been reported in the income statement.

Taking a step back in order to have a complete overview of the situation, the accounting principles provide that some costs have the duty to be capitalised throughout the years, since they generally refer to asset which are known to have the ability to generate revenue during their useful life, such that the company regularly benefits from it. For the same reason then, also their related costs have the possibility to be spread over the corresponding years. The problem that can arise when companies apply this accounting practice, refers to the improper capitalisation of costs. For instance, WorldCom was found to include wages and salaries of its employees as capitalised costs. The same happened for revenue expenses which were treated as capital expenses with the consequence of being depreciated over time. Of course, by capitalising expenditures as assets rather than recording them as expenses related to the current period causes an overestimation of the income section. As an alternative way to conceal liabilities and expenses companies usually play with returns and warranties figures. In fact, it commonly happens that the products sold by an organization, which is involved in a business transaction, are returned because the customer is not satisfied with the delivered items. When this occurs the management team should intervene by recording the related expense in a contra sales account which will negatively influence the net sales represented by the company. The same happens when the company offers its customer warranties on products sold. The idea is that the warranty represents an entity's future potential expense and for this reason it should be accrued as a liability. However, in order to keep a positive income, the management team could adopt two techniques. The first one is to underestimate the warranty liability by reporting a lower value, while the second strategy is to simply omit the recording of the liability within the financial statement. Of course, both of them are to be considered as fraud. The idea behind the unrecording of expenses and liabilities is that perpetrators truly think they can conceal the illicit act in the future years by using alternative income sources such as, for example, the profit from future prices increase. But this unfortunately is not what happens most of the times.

1.6.5 Improper Disclosure

Contrary to what is common thought, financial statement fraud is not just related to the misapplication of the evaluative and accounting criteria, rather it goes way beyond them, since it also considers the modalities in which these are classified, represented, and commented. Therefore, it is not correct to underestimate this category since distortions can arise also because of improper reporting, especially when the attention is exponentially increasing towards the quality of the information disclosed. For instance, additional information is required by law as a supplemental tool to the company's balance sheet and it should be disclosed in the Notes to financial statements. The latter is identified as a company's vital part used in order to explain, for example, how the management team reached the numbers represented in the respective accounts, which evaluation criteria it has been used and also the accounting policies that have been adopted during the preparation process. Stated this, what traditionally happens though, is that all the information regarding estimation of contingent liabilities or company's possible future risks, are purposefully not revealed in the notes. Other times they are just improperly disclosed. The same happens for particular events that have significantly affected the company just after the balance sheet has been closed, but still, before its final approval. Not only, many management teams, who are responsible for the information disclosure and for its accuracy, also avoid reporting the new accounting treatments used for the estimation of item's values and, at the same time, to report how these have influenced and have impacted the balance sheet. As evidence shows then, the improper disclosure of such elements is the most advanced and sophisticated form of fraud, which is still subject to continuous evolution and reworking in order to satisfy the information requirement coming from an increasingly demanding economic environment. For instance, when carefully analysing a company's income statement, the attention could be grabbed by the presence of the *discontinuing operations* item, since it is reported in a different line with respect to *continuing operations*. This separation, in compliance with the regulatory standards, must be recorded in the income statement section when a company is still possessing a business line, which however, is no longer operational or rather it will be sold in the near future (held for sale). Of course, this distinction is essential for the financial statement user's, who, thanks to this accurate representation, will be able to understand which is the continuing income that the company is able to generate and repeat through its operational core activities, and which, instead, is the discontinued one, which has been part of just an extraordinary event. Therefore, by altering this information on the Notes, managers completely mislead user's perception of the company's situation, making it difficult for them to properly evaluate the actual profitability of the company, thus indulging into fraud.

Typical omissions involve also contingent liabilities which represent potential obligations that could materialize in the future only if certain events occur. For instance, when a company is involved in a lawsuit and the third party has a strong case in hand, the former should take into consideration the potential damages that this event could cause. For such reason, the event should be disclosed, and a contingent liability should be booked in the company's balance sheet in order to give a truthful view of the company's financial situation. Therefore, if the potential liability is material, it should be disclosed and if this does not occur such scheme should be categorized as fraud. The improper disclosure can be applied also to many other items, such as foreign investment operations or related party transactions. For instance, the latter has been recognised as one of the most recurring scenarios where information is purposely left undisclosed. About this, a company might be involved in a business transaction with another entity whose operating, or management policies are controlled or rather, significantly influenced by the company or in alternative by a third party in common. Such relationships should be immediately disclosed or else there could be the inherent risk that the business transactions are not conducted on an arm's length basis which could undoubtedly harm the company's stakeholders.

This need to reveal the relationship is related to the fact that the financial interests that a company may have are not so visible to stakeholders and, for this reason, it is necessary for them to be clearly disclosed by those who are aware of them, such as the management team within the organization. For instance, a company facing a difficult financial situation in a specific period could be drawn to the idea of transferring part of the related party's wealth to itself. By doing so, the company's action could be defined to be both an entity's misappropriation of assets and also an improper disclosure of information. Similarly happens when dealing with investment operations, which clearly express the company's future intentions to engage in particular projects. Such projects are mandatory to reveal especially to investors, who are the ones actually investing the money in the company's plans. For instance, expanding in another country could lead the company to face further unexpected risks, and it stand to reason that, it is essential to communicate the matter and enable investors to evaluate their future prospects as well. However, if this type of information lacks to be reported in the Notes, investors would be left in the dark from the company's intentions and managers would not be acting in their best interests as they should.

1.7 Fraud prevention

Fraud prevention is a process that has undergone through several developments during the years. To better understand the evolution, it is worth taking a step back into the 1980s when the financial reporting environment was much less complex than the actual one. About this, it was common thought that when a fraud scam managed to be detected, the only ones held responsible for it were auditors, since CEOs justified themselves stating that they had firmly relied on external auditors, who, in addition, had been paid for this job. Therefore, external auditors were constantly blamed and conducted into courtroom every time their workpaper brought in light some accounting problems concerning the company's accounts. This led auditors to understand that no matter how many frauds they were able to detect, they would still be considered as a mean of risk diversification. To make matters worse, in the same years, companies progressively grew their exposure to liabilities which of course, implied major attention from the auditor's point of view and contributed to increase their terror of being held responsible for any inconvenience. It was clear that this system could not work for any longer and responsibility allocation should have been revised. However, the response to the problem was publicised only seven years later by the National Commission on Fraudulent Financial Reporting (USA), which, after several research, stated that financial statement fraud is a consequence of environmental, institutional, or individual forces and opportunities. Therefore, every company can be easily exposed to fraud, since the mixture of these elements could represent a good opportunity and incentive to perpetrators. For this reason, it became important to shift the spotlight on company's corporate governance, while making sure that in each of them there was the right *tone at the top*, which meant that top managers had to transmit, all over the organization, the right attitude in order to correctly comply with the accounting principles in the financial reporting. This ensured that all employees and third parties were aware of what was and what was not acceptable within the organization. However, relying just on the spread of tone *at the top* as an internal control, turned out to be ineffective since, within the enterprise categories, the ones who suffered external pressure the most were exactly top managers. For instance, this is still something happening nowadays, since the 2020 report to the Nations states that 22% of fraud perpetrators were found to be managers, while just 15% were represented by employees. To contrast this problem, the National Commission of Fraudulent Financial Reporting established the mandatory presence of two key roles within the company: The Board of Directors and the Internal Audit Committee. The former had the responsibility of supervising management activities and in doing so, it also had to ensure that *tone at the top* was actually transmitted. The latter instead, represented an informed body which could oversee the financial reporting prepared by the company's management teams. Therefore, by establishing two intermediate bodies and by stating that fraud begins with the presence of undue pressure in the top management, the NCFFR was indirectly shifting the financial misreporting responsibility to managers at first, followed by BOD and Audit committees. In addition to the introduction of BOD and Audit committees, the NCFFR also led to the definition of standards concerning internal control systems, which are the ones reported today by the Committee of sponsoring organizations (COSO). These standards have subsequently influenced other normative laws, such as the well-known Sarbanes-Oxley Act (SOA) and also crime prevention laws. The former was introduced in 2002 in the US in order to prevent the recurring of other accounting scams after the ones declared by Enron, WorldCom, and Tyco international which had severely undermined the investor's confidence in the market. The law established a mandatory presence of transparency rules when reporting financial information, the constitution of the Public Company Accounting Oversight Board, which aim was to control listed company's balance sheets and also the internal control system's increase. However, even if the law provided for the introduction of sound internal control systems, many have criticised the usefulness of these tools, since the 2020 report to the nation stated that the majority of detected fraud cases were pursued by top managers, who possessed the authority to override such systems. The report, however, showed also that companies which implemented sound anti-fraud systems managed to reduce two times the median loss faced by companies which instead did not arrange for their introduction. The most significant control systems that made the difference, according to the latter report, were codes of conducts; internal audit departments; management certifications of financial statements; external audits of internal control over financial reporting and management reviews. In fact, by ensuring that all the above-mentioned controls existed and were correctly implemented, companies managed to reduce the median loss by 50-51%, which in terms of number corresponded to $200,000-$205,000 totally saved. Not only the report considered the relation between anti-fraud controls and median loss, but it also highlighted how these systems were related to the duration of the illegal schemes, which in five specific cases contributed to uncover fraud in just half of the time with respect to companies which did not implement them. Therefore, in light of the results, just by focusing on the prevention of fraud cases, organizations can benefit under the economic and temporal profile. This is what the crime prevention law proposed, a shift towards prevention rather than on detection, since the major final aim of legislators was, and still is, to prevent crimes.

Great changes have occurred through the years as a consequence of the increased awareness of companies which, day by day, are taking the threat of fraud more seriously. Evidence of this is shown by the 2020 Report to the Nation, which highlights the implementation rate increase of four specific anti-fraud systems from 2010 to 2020. Hotline, Anti-fraud policy, fraud training for employees and fraud training for managers/executives are measures specifically designed to mitigate fraud risks and in ten years their implementation has correspondingly grown by 13%, 13%, 11% and 9% respectively. About this, it is important to highlight that it is not enough for a company to just have an existing and operating internal control, considering that deficiencies could arise even if this is not properly designed, such that it would not allow management or employees to prevent or detect the misstatement on a timely basis. One of the biggest problems related to fraud prevention is generally to convince the management team of the importance of introducing such systems while, at the same time, distracting them from the mere financial aspects and encourage them to look further. About this, who is still hesitant to comply with such preventive systems are mainly small companies, that are also the ones facing different challenges with respect to bigger organizations. The main reasons lie in the lack of resources to put controls into place, but it is also a problem of lack of awareness, combined with too much confidence on employees due to the entity's small size. At this point, it is clear how Fraud can hit organizations straight in their bottom line, but while big corporations still manage to withstand several figure fraud, small companies or also non-profit organizations might never recover from them. For this reason, in order for companies to survive in today's competitive marketplace they should start taking a proactive role rather than just being reactive and start fighting this phenomenon. Of course, when thinking about fraud prevention, the first thing that comes to mind are internal controls. In fact, if the procedures that control the way in which things are done within the company are set up properly fraud will never occur. This of course is what should happen in practice, but actually the truth is that perpetrators are always ready to find a way to circumvent controls and accomplish their own agendas. Each day organizations face high numbers of risks that are potentially harmful and that can cause them serious damages. Among these risks what usually goes unnoticed is the issue concerning vicarious liability. In fact, not only companies can be held responsible for illicit actions committed, but they can be partly responsible also for illicit acts committed by their employees, if performed in order to benefit the company. Linked to this there is also the risk of getting the reputation back as happened, for example, to Arthur Anderson's company, who was once known to be among the best accounting firms. In addition to this, it is worth also considering the emotional toll that fraud can cause, since the final ones who generally suffer the consequences are employees and families who are not involved in the company's fraudulent action. It stands to reason that all entities need a robust fraud prevention program considering how critical this is for the long-term existence of a company.

Fraud prevention nowadays is a requirement. In an interview publicised by the "Executive roadmap to fraud prevention ad internal control: Creating a culture of compliance" book, Joseph T. Wells, the founder, and chairman of the Board of the Association of certified fraud examiners, provides some comments on fraud prevention. In particular, to the question of what corporate executives must do and that they are still not doing in order to prevent fraud, he answers that the most important thing is to have a proper *tone at the top* below the executive level. For instance, if executive does not walk the talk, then also employees will not have a proper behaviour within the organization, simply because it is necessary to lead by example. Secondly, Mr. Wells states that internal controls are not the root cause of fraud and for such reason, they cannot be used as the only fraud prevention tool. In fact, one of the main causes of fraud occurrence is employees' dissatisfaction with the workplace conditions. Therefore, great importance should be given to the way in which employers treat, respect, and compensate their respective workers. Last, Mr. Wells analyses how prevention is instituted outside the United States in relation to the number of fraud cases occurred. About this, what the chairman affirms is that Europe is facing less fraud cases because of its better care towards underprivileged citizens, which is the consequence of the almost non-existing gap between the "haves" and the "have nots". Japan and China are also known to be countries where fraud is less widespread, probably due to their cultural prohibitions against dishonesty. On the contrary, in Latin America the great reliance on drug trade as a mean to fuel the economic system has brought to fraud's rapid expansion

2 Chapter 2 - Integrating control with Enterprise Risk Management

The internal control term has been mentioned several times throughout the paper's sections and each time it has been defined as the needful tool in order to prevent corporate frauds. Despite this, nothing has been said yet about its role and its potential. Therefore, the objective of this chapter is to analyse the internal control system concept and its role as a supporting tool in order to prevent the occurrence of fraudulent activities. Furthermore, in light of the changes within the business environment and the changes on risk's complexity, the chapter will focus also on the risk management concept. As the next chapters will show, risk management and internal control are perfectly compatible. However, when dealing with such topics, one of the main difficulties lies in the lack of a clear and unique definition of the internal control term, especially within the Italian reality. In fact, the term assumes different meanings in relation to the concept to which it is applied. Generally, within the public sector, internal controls' objective is to verify compliance with laws, regulations, and contracts. In the financial sector instead, the term is gradually taking on a specific definition, thanks also to the Italian Bank's claims. About this, bank's supervisory instructions require credit institutions to comply with capital requirements and to use control systems in order to ensure an adequate management of the market risks. On the contrary, in the private sector the situation is completely different. There is no clear vision and definition of the internal control systems. This is the reason why many companies are not yet equipped with an adequate structure for their needs and many others are not even considering it. In fact, in Italy there is no reference model to follow in order to implement and project a sound control structure. For such reason it is necessary to make references to overseas literature and legislation. For instance, in the United States, the Committee of sponsoring organizations of the Tredway commission (COSO) already defined the internal control system concept in 1992, after the occurrence of several scams that took place in late 80s. The committee, formed by a federation of the American Accounting Association, American Institute of CPAs, Financial Executives International, Institute of Management Accountants, and Institute of Internal Auditors, issued the COSO report *Internal control- an integrated framework*, with the objective of providing a clear definition of control and a reference standard for those companies willing to implement their internal control systems. In addition, the commission's aim was to improve the quality of company's financial reporting by setting major focus on corporate management, ethical standards, and internal controls. Later on, in light of the changes to the environment, precisely in 2004, the COSO body decided to also issue the Enterprise Risk Management framework in order to improve organizations' approach to risk management. However, it is worth stating that the Enterprise Risk Management-Integrated Framework (ERM) should not be considered as a replacement of the COSO Internal Control-Integrated Framework. On the contrary, the two are perfectly compatible and are based on the same conceptual foundation. As the next chapters will show, the ERM represents a broader framework which incorporates the internal control system. Therefore, COSO reports are nowadays the only example of literature to deal with internal control and risk management that have gained broader acceptance by organizations. Before entering into the definition of the internal control term and into the analysis of the ERM's components, it is important to review the main stages that have contributed to strengthen the internal control's importance within the Italian corporate governance context.

2.1 The origin of Internal control systems

Many are the sources that deal with the concept of internal controls, and many are the points of views by which it has been studied, in relation also to the evolution of its role within companies' internal control systems. The first time that the internal control system term appeared in the Italian legislation dates back to 1998 with the D.Lgs. n.58, known also as Testo Unico Della Finanza (TUF). In particular, art. 149 stated that the Board of Statutory Auditors had to comply with the duty of supervising company's internal control system's adequacy. Hence, until then, the Board of Statutory Auditors had the responsibility to supervise the company's administration and no other instruction was given with respect to internal controls. Therefore, the role previously covered by the body was totally different from the role of stating the adequacy of company's internal control systems. In fact, the civil code, precisely art. 2403, provided that the Board of Statutory Auditors had the duty to supervise company's compliance with the law and with the by-laws, to verify company's correct bookkeeping, to verify the match between the financial statements and the book's results. All these tasks were equally valid for each company that had an obligation to appoint the Board of Statutory Auditors. However, this task assignment created many criticisms. In fact, it was common thought that such tasks overlapped with the activities carried out by audit companies and that no instruction was given on the modalities to implement such controls.

In the wake of the experience gained in the field of internal controls, especially by the Anglo-Saxon countries, in Italy during the 90s, it emerges the need to adopt adequate internal control systems in order to ensure a proper business management. About this in 1996, the National Council of Chartered Accountants issued the "*Principi di comportamento del Collegio Sindacale*" that provided for the first time a definition of the procedural process to follow and the instructions on the documentation needed in order to evaluate the companies' internal control systems and its accounting organisation. In particular, the norm 2.5 stated that the Statutory Board of Auditors had to evaluate the internal control systems' reliability through the activities of:

- The expression of a preliminary judgement concerning the system's reliability.
- The documented detection of procedural cycles and the identification of the system's main weaknesses.
- Sample verification of the control activities' actual operating.
- Final evaluation of the internal control systems and subsequent planning on various balance sheet items' checks.

However this acted only as a regulatory contribution since what mattered the most was the above mentioned D.Lgs issued in 1998. In fact, the latter redefined the role and the tasks of the Statutory Board of Auditors in listed companies. Furthermore, it was the first time that the importance of the internal control system in corporate governance was finally made official at the legislative level. The TUF has redefined the regulation of listed companies' surveillance and control systems by separating:

- The statutory board of audit supervising activity, with its related control power over the company's management.
- The audit company's control activity which is reserved only to those companies registered in the Consob register.

Two particular articles within the TUF, albeit in a limited way, are specifically related to the internal control activities and they represent the very first legislative intervention to focus on such issue. Hence, the Board of Statutory Auditors is expressly assigned a duty of supervision both on the company's internal control systems and on the accounting administrative systems' adequacies. Following this trial, in 1999 the National Council of Chartered Accountants issued the "*Principi di comportamento del collegio sindacale nelle società di capitali con azioni quotate nei mercati regolamentari*" with the aim of supporting and guiding the Statutory Board of Auditors through the control systems' performance. In the same year, the "*Comitato per la corporate governance delle società quotate*" of the Italian stock exchange issued a self-regulatory code in order to provide listed companies with an adequate reference model to manage the correct control of business risks. Within the code there is a specific paragraph that deals exclusively with the internal control system, and it represents it as the qualifying element for a good business management. In particular, art.9.1 of the code defined internal control as the set of processes which aim was to directly monitor the business operation's efficiency, the financial information's reliability, the compliance with the law and the safeguard of company's assets. Therefore, until 1980s the internal control system was simply part of a "fulfilment culture", such that it was perceived as a mere tool to guarantee compliance with the law. Furthermore, it was considered also as the tool able to contrast any internal or external action that had contravened the rules set by the company. Therefore, Internal control system has always been perceived as something not related with real business activity especially because it was exercised by organizations which were totally different from the ones carrying out operating activities. Later on, the concept was strengthened by the so-called "command and control" idea, which provided for a mere ex post control in order to ensure employees' work compliance with the orders given by managers.

What partially changed societies' internal control system idea, was the introduction of the *directional control* concept. In particular, companies' management teams had the duty to verify that the internal management processes were actually effective for organizations' objectives achievements. By looking at this perspective, it was clear that control was actually being considered as a part of the strategic planning processes, which comprised goal setting processes, resources setting processes and activities definition processes in order to achieve predefined objectives. However, it was just between the 80s and 90s that the internal control concept diverted from the idea of being a mere fulfilment tool and started to be considered as an important business tool. This idea was enforced especially by the internal control combination with the risk assessment and risk management concepts. By then, internal control systems were definitely part of business activities since they represented important management tools able to handle business risks with positive effects on businesses' performances. The consequence of this particular change in the internal control's idea also determined a change towards the subjects responsible of such system. In fact, it is clear that if the business risk management processes, which are pursued through the internal control systems, impact on the company's operational performances, then the function will be proper of the ones who manage the company. Hence, management teams were not only responsible for achieving the planned results, but they were also responsible of identifying the risks that could compromise the objectives' achievement. The ability to prevent risks and to find an acceptable risk level has become a real managerial resource.

2.2 The COSO Internal Control Integrated System

After a brief outline of the legislative sources that have shaped the internal control system, it is worth introducing a definition of the concept in order to identify each system's component. One of the most important definitions has been provided by the COSO body in 1992 and it has been subsequently revised in 2013 in order to reflect the changes in the business and operating environment and also to clarify the internal control's effective requirements. The definition stated what follows: "*Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance*.". This definition reflects several important concepts which are worth analysing in order to understand how the system is structured and works.

First of all, the internal control system is defined as a *process* which means that it is not an end to itself, but rather a mean to an end. Furthermore, it is defined as a dynamic and integrated process rather than being classified as a serial process. Secondly, it is geared to the achievement of objectives in several categories such as operations, compliance, and reporting. Each of these objectives will be deeply analysed in the next sections. Furthermore, the definition introduces the concept of *reasonable assurance* which diverts from the concept of *absolute assurance*. In fact, any sound internal control system is able to provide just a good dose of security towards objective's achievement to both senior management and board of directors. This of course is an intrinsic limit that refers to each internal control system since the process is pursued by people and it cannot prevent wrong decision making or system's rules circumvention. Since the internal control has been defined as a managerial tool, the first ones to benefit from it are managers. However, also stakeholders can have a reasonable assurance that their interests are protected and considered within the business activity. By looking at the COSO definition it is also clear that the internal control activity is not something different than the other managerial processes. In fact, the system does not involve only bodies in charge of control, such as Auditors and Board of Statutory Auditors, but it also represents a fundamental component of the management system. For instance, in the self-discipline code released in 2006, precisely in the comment to principle n.8, the Corporate

Governance Committee underlines the importance of the Board of Directors when dealing with the internal control system. In fact, the body has the responsibility to adopt a system which is adequate to the company's characteristics. It is worth also mentioning that within listed companies there are other bodies that participate in the rule and internal control system definition processes. These bodies are represented by the Internal Control Committee, Internal Auditors, risk management and the compliance function. These bodies support the Board of Directors in the above-mentioned practices. As the COSO definition recalls, the internal control systems' main objectives are divided in to three particular categories:

- Operations objectives, which aim is to guarantee the efficacy and efficiency of entities' operations. In addition, they ensure decisions compliance with the directives and the business' mission. Furthermore, they offer an adequate level of corporate assets' safeguarding.
- Reporting objectives, which aim is to guarantee not only data reliability but also the reliability of the company's financial and non-financial reporting.
- Compliance objectives, which aim is to guarantee business activities' compliance with the law, with the statute, with rules and with the principles of correct administration.

The three together are considered as businesses' common objectives since they are supported by universally shared principles such as compliance with the rules, reliability of corporate information and the effective and efficient use of the business resources. In addition, each of these objectives if not adequately pursued can lead to company's economic losses and value disruption. For instance, the control over the cost-effectiveness of the entities' activities, provides for the detection of coherence between the actions pursued by entities' members and the entities' global mission. The two are constrained by the efficient use of resources and the optimization of its risk profile. For what concerns the internal control, which object is the achievement of the financial reporting goal, it is clear that since the latter is based on norms and laws issued from outside the entity, it enables the company to keep a good reputation. Therefore, internal control should be directed towards the information issued by the company such as financial statements, non-financial documents, extraordinary accounting situations and so forth. Reliability of such information can be valued in terms of existence, completion, accuracy, and timeliness of information.

Finally, compliance control has the task to ensure that all people who are empowered with decision making actually operate in compliance with the laws and the rules set by the company or by external authorities. For instance, by looking at the external legislation, an Italian company must operate in compliance with the civil code, with the tax legislation, with TUF dispositions and so forth. On the other hand, when looking at an entity's internal environment, in order for it to operate in compliance with the internal rules, the management team must respect, and enforce others to respect, entities' conduct codes or alternatively the group's accounting principles.

However, before entering into the core of the topic it is worth explaining the reasons that led the COSO body to update the 1992 internal control framework. As it is common knowledge, since 1992 the world has undergone through significant changes such as the emerging of globalised markets, shifts in business models as well as a greater use of outsourced service providers. Not to mention the intensified regulations which have generated higher expectations among stakeholders and regulators in terms of risk management, governance oversight and fraud's detection and prevention. Therefore, in light of these changes the COSO body decided that there was a greater need for competence and accountability. Thus, in 2013 the body issued the "Internal control integrated framework" (ICIF). Despite this new introduction, the board stated that the principles and the concepts which were embedded in the original framework would still be relevant today. While the original framework implicitly reflected the internal control's core principles, the updated report explicitly states them in order to increase management's understanding. The following table represents the seventeen principles associated with the five components. The management team believes that each principle adds value and acts as an important tool to help internal control implementation within entities.

17 Principles associated to the Internal Control Framework 2013

Control Environment	1) Demonstrates commitment to Integrity and ethical values 2) Exercises oversight responsibility 3) Establishes structure, authority and responsibility 4) Demonstrates commitment to competence 5) Enforces accountability
Risk Assessment	6) Specifies suitable objectives 7) Identifies and analyzes risk 8) Assesses fraud risk 9) Identifies and analyzes significant change
Control Activities	10) Selects and develops control activities 11) Selects and develops general controls over technology 12)Deploys through policies and procedures
Information & Communication	13) Uses relevant information 14) Communicates internally 15) Communicates externally
Monitoring Activities	16) Conducts ongoing and/or seperate evaluations 17) Evaluates and communicates deficiencies

Figure 6 "COSO framework's 17 principles"(Source COSO Internal Control-Integrated Framework, Executive Summary, 2013)

As the table shows, there is an increasing attention towards fraud risk. This emerges in the eighth principle which also outlines the measures that managers should take in order to manage this type of risk. Furthermore the 2013 framework highlights the importance of general controls over technology. In fact, technology changes can affect the business activity and this in turn can affect the type of controls carried out within the company. For instance, there are two types of situations which can depict the relationship between control and technology:

1) The business' internal processes use technology as a supporting tool. Therefore, in this case the monitoring process is used to avoid breakdowns or deficiencies of technology.
2) Internal controls are all automated thanks to technology.

It is important to focus on such aspect since the number of organizations which rely on technology is constantly increasing.

Another interesting concept introduced with the latest report concerns the reporting activity. In fact, the scope of reporting objectives goes beyond the financial information. As a consequence, the framework expands the types of reporting by adding internal financial, internal non-financial, external financial and external non-financial reporting. There is more concern towards non-financial reporting since it is growing ever more important. In fact, nowadays stakeholders are more sensitive towards non-financial information. For instance, just think about companies' commitment to sustainable development or their attention towards CSR (corporate social responsibility) and how this can clearly affect stakeholder's investment decisions.

However, since this report is just an update of the previous version, there are also stable elements which have not changed. First of all, the internal control's core definition which is still the same as the one provided at the beginning of the chapter. Secondly, the cube's structure and its dimensions which are still the same as the original version. But the most important thing which hasn't changed is the criteria used to assess the effectiveness of the internal control system. In fact, for the management to conclude that its internal control system is effective, all the five components and all the seventeen principles must exist and function. To ensure the existence, the management team should verify that the given principle or component is present in the design and implementation of the organization's system. While to assess its functioning, it should verify its continuous existence in the operations. Linked to this, the 2013's framework also focuses on the "deficiency" term. In fact, the report states that a major deficiency exists when an internal control's deficiency affects the entity's ability to achieve its objectives. Members in charge of using professional judgment in order to understand whether a specific principle or component is not functioning well or rather whether the five components are not operating together are managers.

Stated this, it is now important to focus the attention on the five integrated elements which compose the internal control system according to COSO framework. Their relationship with the above-mentioned objectives is represented through a cube shape which comprises also a third dimension such as the organizational structure of the entity. The latter involves different types of organizational structures such as operating units, divisions, function, and operating level. Furthermore, the framework sets out seventeen principles which role is to support the organization in achieving an effective internal control system. These principles are drawn from each of the five components, and they represent the fundamental concepts related to them. Therefore, starting with the framework's five components, the internal control system can be subdivided into:

- Control environment
- Information and communication
- Control activities

- Risk assessment
- Monitoring

In the next chapters each of these five elements will be analysed in relation to the ERM's framework in order to understand their specific role within the system.

2.3 The Enterprise Risk Management framework

The very first professional applications of the C.O.S.O IC-IF (internal control integrated framework) highlighted several difficulties in the model implementation, especially within the risk assessment component. In fact, entities had to face several problems from a conceptual and operational point of view so as to make *risk self-assessment* implementation very complex. While the framework was helpful in reducing risks around fraudulent behaviours there was no way to actually identify and assess which types of risks the organization needed to put controls around. This represented a very critical aspect since all corporate governance codes had immediately detected the importance of a management independent risk assessment. After 12 years from the issue of the first standard, the COSO body published the final version of the "*Enterprise risk management - conceptual framework*". This was not the only reason though. In fact, following events like Enron and WorldCom, a heightened concern, and a call for risk management, prompted COSO to update the original COSO framework. This document represents a reinterpretation of the concepts expressed within the original paperwork "Internal Control-Integrated framework" and it also emphasises the concept of risk assessment as a precondition in order to plan sound internal control systems. The final aim is to improve the entities' risk management process in order to meet the demand of an evolving business environment. However, this was not the last version since in September 2017 COSO issued an updated ERM which title was "Enterprise risk management-Integrating with Strategy and Performance". This framework is not just focused on preventing value erosion and risk minimization, rather it highlights the importance of strategy setting and opportunities identification to generate and maintain value. Therefore, the framework better integrates the relationship between risks, performance, and strategy. Considering that each element affects the other two, handling them separately is actually impossible. It is important to highlight that the 2017 framework gives a reworded version of the 2004 COSO framework's components and it outlines twenty principles which contain the same concepts as the ones included in the 2004 framework. Of course, the main reason to implement such system is its ability to support value creation by reducing the likelihood of downside outcomes while increasing the upside ones. Although this model has attracted many criticisms, ERM is still a widely accepted framework that can be used in many different environments worldwide. Enterprise risk management, also known as EMR, has been defined as follows: "*Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*". This definition reflects some of the following fundamental aspects of the ERM framework:

- It is a continuous and pervasive process that affects the entire organization.
- it is carried out by members who occupy positions at all levels of the corporate structure.
- it is used for strategy formulation.
- It is used throughout the organization: both in its individual activities (at each level and unit of the structure) and in its overall activity. It includes a risk vision that considers the company as a whole.
- It is designed to identify potential events that could affect the business and to manage the risks within the limits of the acceptable risk level.
- It is able to provide reasonable assurance to the board of directors and management teams.
- It is capable of achieving objectives relating to one or more distinct categories, which can overlap.

This definition is intentionally extensive, and it contains the key concepts which are fundamental to understand how companies must manage risk; it provides the basic criteria to be applied in all organizations, whatever their nature is. It focuses directly on an organization's specific goal achievement, and it provides the criteria to evaluate the effectiveness of ERM system.

The relevant objectives' categories for the ERM are wider with respect to the previous principles since they also include the strategic objectives category. Furthermore, the document includes the eight components that constitute the ERM system such as: Internal Environment, Objective setting, Event Identification, Risk assessment, Risk response, Control activities, Information and communication and Monitoring. Before going deep into each of these concepts it is worth mentioning again that ERM framework does not replace the C.O.S.O *IC-IF*, but rather it acts as an extension and completion document.

But what is the relationship between ERM and internal control? Perhaps this is one of the most opened questions. In a response to a frequently asked question the authors of the 2017 framework answered as follows: "*Internal control is positioned within the Updated Document as a fundamental aspect of enterprise risk management. The two COSO documents complement each other, with neither superseding the other. The updated document will focus on requisite areas that go beyond internal control; however, the Internal Control—Integrated Framework remains a viable and suitable framework for designing, implementing, and conducting and assessing the effectiveness of internal control and for reporting, as required in some jurisdictions.*"[10] Therefore, while the ERM system gives indications about the strategy, internal control is pursued at a more tactical level. For such reason, the ERM model comprises the five main components of the 1992 COSO IC-IF and it integrates them with other three new components which are: objective setting, event identification and risk response as the following figure shows.

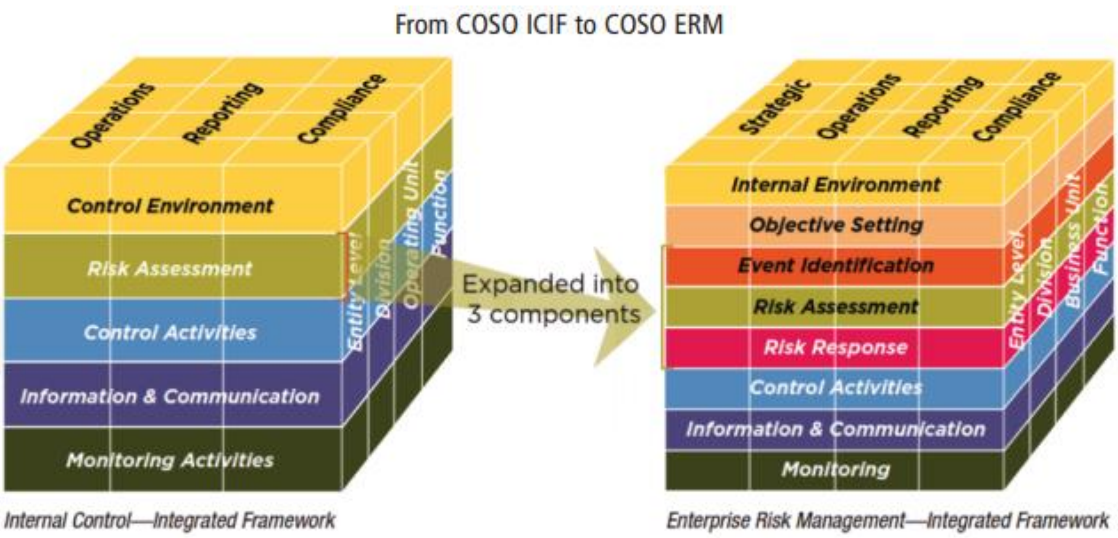

Figure 7 " IC-ERM frameworks" (Source Strategic Finance, April 2014, Leveraging effective Risk Management and Internal Control)

It is important to highlight that ERM is not a strictly sequential procedure, since each component can affect the others to the same extent, regardless of the process' sequence. In fact, there is a direct relationship between objectives, that is what a company strives to achieve, and the components of the ERM, which is what is needed to achieve the objectives. As the above figure shows, this relationship is schematized in a three-dimensional matrix in

[10] Protiviti, *The Updated COSO Internal Control Framework*, frequently asked questions, April 2014

the shape of a cube. The four categories of objectives - strategic, operational, reporting and compliance - are represented in the columns of the cube, the eight components are instead represented in the horizontal lines, and the operating units of the organization are represented by the third matrix size. This scheme reflects the extreme flexibility of the model since it can be applied: to the whole corporate risk management process, or separately to the individual categories of objectives, the components, the individual operating units, and the individual sub-units of the latter. Also, each person working in an organization has a certain responsibility in the ERM system. For instance, the CEO bears ultimate responsibility. The management team promotes the risk management philosophy and the compliance with the acceptable risk level. Furthermore, they have the responsibility to manage the identified risks in line with the risk tolerance level. Generally, the Risk Officer, the Financial Director, the Internal Auditor perform key tasks to support the risk management, other people instead perform purely executive tasks in accordance with the directives and the protocols. The Board of Directors plays an important role in overseeing the business risk management process and contributes to the acceptable risk level determination. Finally, several external parties, such as customers, suppliers, partners, external auditors, and financial analysts often provide useful information for the smooth running of the risk management process, but they are not responsible for its effectiveness, nor are they part of the process itself.

2.3.1 Internal Environment

The first ERM component, *Internal environment*, has been defined as: "*The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate*".[11] It is not a surprise that this component represents the first section of the ERM cube. In fact, an entity's internal environment has a significant impact on how ERM system is implemented and functions on an ongoing basis. Hence, the latter represents the context in which the other ERM's components are applied. The framework highlights several elements which compose the internal environment:

1. The Risk Management Philosophy

   The risk management philosophy has been defined as follows "*An entity's risk management philosophy is the set of shared beliefs and attitudes characterizing how*

[11] COSO, Enterprise Risk Management, Executive Summary, Sep.2014

the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities”.[12] According to its industry sector, to its history, to its economic situation and based also on its attitude towards risk, each company has its own way of managing risk. However, it is fundamental for the risk management philosophy to be shared and understood by all entity’s members. In fact, behaviours which divert from the entity’s philosophy could be very harmful for the company’s business activity. Furthermore, philosophy is reflected in each action pursued by managers while running the business, in the so-called *Risk appetite*. In fact, the latter represents the amount of risk that the company is willing to accept while it tries to achieve its predefined objectives. Despite the way in which it is defined, (using qualitative or quantitative approaches) *risk appetite* influences the entity’s culture and its operating style. There are three specific reasons why firms tend to identify risk appetite and therefore to set limits to the business activity’s risks. First of all, management’s risk level definition is part of their ordinary approach to risk. Secondly, it is a specific way to diversify risk exposure. By doing so, managers avoid risk concentration within a single business area and manage to adopt a systemic perspective in order to manage risk. In fact, the risk appetite is the result of management’s choice in evaluating the company in its entirety. Last but not least, it permits the company to define a risk tolerance level which is related to the achievement of a specific return objective. As everybody knows, higher risks will generate higher returns.

2. Integrity and Ethical values of the organization

   Integrity and ethical values are fundamental elements within the internal environment since they significantly affect the planning, the managing, and the monitoring of the other ERM’s components. These elements concretely translate into “codes of conducts” which represent the set of rules that the company intends to respect. It often happens that companies issue their own written code of conduct in order to clarify their inspiring ethical principles and also to share their Risk management philosophy. About this, the latter involves all the sets of beliefs and attitudes that characterise the way in which risk is considered within any organizational activity. Ethical values and risk management philosophy must be implemented within the company and not just communicated. In fact, this code can

[12] COSO, Enterprise Risk Management, Executive Summary, Sep.2014

be very effective within each company, not only if supported by sanctions in case of its violation, but also if properly internalized by its employees. For such reason companies should find the right incentives in order to enable such internalization. In fact, by internalizing the code, employees demonstrate their understanding and their approval of the respective document. As an example, PWC is committed to operating within a framework of five core values such as act with integrity, make a difference, care, work together and reimagine the possible. The company makes sure that all its employees are aware of how to behave in a manner that is consistent with its values. To do so, the global company organises training courses for each employee through the L&D (Learning and Development) service line together with specific platform access. However, the best way in order to spread an ethical culture and to promote a message of behavioural conduct is for managers to lead by example. About this, studies have underlined that people within organizations tend to behave in the same way as their direct managers behave, since due to their role, manager's actions are highly visible to all entity's members. Ethical value identification is a very accurate process since it requires the settlement of different types of interests (clients, suppliers, personnel, society). Both ethical behaviour and integrity are part of the entity's culture. The latter in fact, is a dynamic concept that evolves in relation with the entity. It codifies the organization's behaviours, values, and any other communication activity. The spread of a particular culture within the company leads to the existence of team members who work to achieve the same objectives and who internalize the same reference values. Of course, these values should be transferred also to all new joiners. Therefore, a company can manage to survive only if provided with a culture that comprises values which are able to represent not only the company's actual behaviour, but also the past and future one. Although these values are totally intangible, they strongly determine the company's way of being. According to Dyer G. jr[13] an entity's culture may occur in many different ways such as:

- Through external symbolic expressions. For instance, verbal (language), behavioural, material (logo, dress code)
- Through perspectives, such as rules followed by the group in order to solve a problem.
- Through attitudes, towards the environment, towards colleagues.

[13] G. Dyer jr, *Culture and continuity in family firms, in family business review*, vol 1 spring 1988 p.37-50

3. Human capital skills

   The control environment is characterised by human capital's skills and for such reason it is fundamental to ensure the existence of a match between required skills and assigned tasks. Therefore, companies adopt several processes in order to retain and attract competent individuals that possess the necessary skills to carry out predetermined tasks. Companies usually apply training policies in order to give employees an insight of what the entity is expecting from them and what is the level of performance required. Not only, companies might try to retain their workers by offering rewards or promotions and by showing their will to encourage advancement.

4. The organizational structure.

   Since the company is an organised system made of people and knowledge it is necessary to have an adequate structure in order to connect all different elements. An entity's organizational structure is characterised by several features such as: work division, grouping, coordination mechanisms, power delegations and human resources management policies. In order to have a sound organizational structure each of them should be linked together.

   - Division of Labour

     This concept has been studied by many important scholars which gave their contribution on the topic. First of all, work division provides for the breakdown of processes into elementary activities with the aim of grouping them into tasks by following a logical criterion. Secondly, the tasks are assigned to people who possess a defined role within the entity. Finally, each person is assigned to a specific job position. About this, H. Mintzberg[14] in one of his inspiring books offers an important contribution to the topic by introducing the concept of *specialization*. According to the author, specialization can be vertical or horizontal. In the first case the job position is assigned few activities, which sometimes are homogenous and others not. In the second case instead, the job position has very few authorities which do not permit decision making.

   - Grouping

     This concept concerns body's grouping, and it can be realised in different ways. For instance:

[14] Mintzberg H. La progettazione dell'organizzazione aziendale, il Mulino, 1985

    - Based on the business process input which relates to the technology used or to the function of the implemented activities (marketing function, human resource function and so forth.)
    - Based on the output of business processes such as the product, the market, the types of clients or the geographical area where the entity operates.
    - On numerical base, when the bodies are grouped into teams which work simultaneously on the same activity.

- ➢ The hierarchy

  Various levels of grouping are related with different levels of authority which determine the entity's corporate hierarchy. An organizational structure with very few hierarchical levels is considered as *flat.* However, what differentiates this organisational model is its direct relationship between the top management and the operating bodies which speeds up the decision-making process while minimising communication errors.

- ➢ Coordination Mechanisms

  Coordination mechanisms are used to connect all the entity's different functions. Concretely, they deal with the entity's lay out, with the objective's communication and with the formalization of work activities, skills, and knowledge. For instance, the latter activity involves the definition of organizational charts, job descriptions and working procedures. Therefore, it is a dynamic process since the high mutability of the context and the external environment's rate of change require a flexibility in the organizational structure. In order to do so, the relationships within the entity's working groups should be consolidated. There are several methods in order to achieve such objective, for instance:

    - ➢ The implementation of task force to solve specific problems.
    - ➢ The creation of connecting positions.
    - ➢ The creation of integrating positions which are endowed with a certain authority over the bodies involved.

5. Models of responsibility and authority assignment.

   Delegation power and all the activities which assign power have an important role within the organization. These processes provide for the definition of authorization procedures, and they encourage entity's members personal initiatives. In order for responsibility and authority assignment to be effective it is necessary that:

- The entity's objectives are known and shared by all the organization's members.
- That power and responsibilities are attributed within the limits of the objectives to be achieved.
- That power and responsibilities' transfer are constantly monitored by the top management who has the final role to approve the made decisions.

For instance, an entity who is willing to increase the gross operating margin by 5% will have to communicate this objective to all its members. Once this is shared through all the organization, then the top management may be able to delegate price increase power to the marketing department manager while constantly monitoring the margins.

2.3.2 Objective setting

As the second element of the ERM model, *Objective Setting* represents the starting point of the entity's planning activities. By setting the main objectives the entity will not only be able to effectively identify potential events, but also to evaluate risks and define the methods to properly address them. What is extremely important is to ensure that the objectives are actually aligned with the level of acceptable risk identified by the company. The objectives defined and strategically pursued by the company substantially affect the organisation's actions. About this, strategic management is a process that starts by defining the company's mission which enunciates the company's purposes. Therefore, the mission defines the enterprise's field of activity and the reasons of its existence. For what concerns the objectives instead, they can be divided into several categories:

- strategic objectives which give a general representation of what are the corporate governance lines, and which must comply and support the entity's mission.
- related objectives which define the methods through which strategic objectives can be pursued.
- Specific objectives which define the guidelines to be adopted at a management level.

For instance, to clarify what related objectives are, if a company's strategic objective is to increase its market share within the international context, then the related objective could be to engage in product differentiation. By doing so the company could promote its new brand in new markets. At the same time though, the specific objectives could define the objectives that each business activity-unit should pursue. It is important to highlight that usually mission and strategic objectives are stable over time, while strategy, related and specific objectives need to be constantly adapted to external and internal changes. As mentioned previously, the related objectives to which the model refers are three: operating, reporting and compliance.

The operating objectives concern the effectiveness and efficiency of the activities carried out by the company. They typically refer to activities of the operating cycle that, within the industrial sector, are defined as purchase, production, and sale activities. It is important to underline that this objective category must be adequate with respect to the reference context and the forces that act on the entity's competitive position. In fact, competitor's behaviours and characteristics can affect the entity's objective definition, especially the operating ones. For instance, typical operating objectives are performance achievement, profitability achievement, protection from any resource loss. Therefore, companies must clearly identify them and express them through measurement criteria in order to be able to verify their achievement through time.

Reporting objectives on the other hand, related to the preparation of internal and external reports (accounting and not) which contain accurate and reliable information. From an internal point of view, they allow the company to benefit from a support in the decision-making stage and during the monitoring of the performance results. From an external perspective instead, they represent an important communication tool towards all stakeholders.

Compliance objectives instead, refer to the fulfilment of laws and regulations introduced by the entity. Generally, normative requirements represent the minimum level to which companies refer when defining compliance objectives. However, companies can overcome the minimum threshold by introducing new parameters based on the companies' characteristics and on the competitor's actions.

It stands to reason that, the ERM model if properly applied, can enable management teams to establish with reasonable assurance whether reporting and compliance objectives are correctly pursued. For what concerns operating objectives instead, they cannot be positioned under the company's total control since they are deeply influenced by the surrounding environment. Therefore, it is important to highlight that ERM's role does not consist in the definition of the objectives that companies should achieve, rather its role consists in the alignment of the entity's mission with the strategic objectives. In fact, the mission is the mean through which companies communicate the purposes they want to pursue. It defines the entities' field of activity and the reason of their existence. Basically, the mission is what makes a company unique with respect to other organizations and it guides governance and management decisions. However, the alignment should consider risk appetite as well. About this, each company should define the amount of risk that it is willing to take entirely. Of course, there is no "standard" risk appetite, since all companies set different objectives, have different missions, and consequently have a diversified risk appetite as well.

2.3.3 Event identification

The ERM model identifies *Event Identification* as the third element of the process. If for any reason potential events occur, they could deeply affect the company's ability to realize its strategy and achieve its predefined objectives. Such stage is fundamental since it enables the company to evaluate the risks and the response to the risks. About this it is important to state that, risk and uncertainty are two different phenomena. According to the financial discipline logic, only the risk element is able to affect people's welfare. As a consequence, uncertain events can exist even without risk, which means that not knowing what will happen does not affect in any way people's welfare. By focusing now on uncertain events which determine risky situations, it is possible to make a further distinction between risks and opportunities. About this, risks can be defined as the ones requiring evaluations and answers since their occurrence could cause entities a negative impact on their results. On the other hand, instead, opportunities can be defined as potential events which could generate positive results. The latter should be monitored by the management team which should be able to rapidly identify and pursue them. About this, the report issues the following indications:

- The entity should identify the events and understand the existing interaction between the determinant variables. For instance, when a company is placed in the middle of the supply value chain it should consider that the demand highly depends on its major client's economic performance.
- The events that can affect the company have an external or internal origin. The firsts involve several company's opportunities or threats, while the second ones involve company's week or strength points.

- Event identification is a very delicate process since even events with low occurrence probability should be considered. Especially if their impact is determinant for the company's objective achievement.

The external environment encompasses the whole range of social, economic, political, technological, ecological factors which affect the company's decision making and its results. About this, Robert Grant[15]underlines that in many cases the company's reference external environment is represented by its industry and for such reason, *event identification* cannot ignore the existing relationship among its competitors, clients, and suppliers. Another scholar, Giorgio Pellicelli[16] gives its contribution to the topic and subdivides the environment into macro environment and microenvironment. While the first one involves several variables on which management teams can't act, the second one comprises variables which directly interact with the company such as clients, suppliers, and markets. To analyse the macro environment the author, suggest the use of the PEST analysis which is a tool that considers the impact of political, economic, social, and technological events. There are several methods in order to identify potential events and companies usually mix up different methodologies which enables them to consider both past and potential events. About this the main methods to calculate potential events are the following:

- Brainstorming. By elaborating and integrating the ideas of people who possess some knowledge on the topic, there is the possibility to identify possible future events.
- Delphi method. The process starts with the collection of several opinions among experts on a probable event occurrence. Each expert will be given a survey and each of them will have to answer without knowing the other colleagues' answers. The collected answers will be then used to fill in another survey and this continues until a general consensus is met.
- Historical series analysis. Drawing projections from statistical series of historical quantitative data
- What if analysis. This is one of the most used methods. It is used to analyze future scenarios and understand the effects of possible events.
- Internal analysis. Potential events are identified by integrating external information with internal information which is collected through meetings.

[15] Grant R.M, L'analisi strategica per le decisioni aziendali
[16] Pelliccelli G., "strategia" in management tomo 3, La repubblica 2005

- Collection of data on losses. Through the collection of past events data which have generated losses the management team will decide whether to focus on the root cause of the loss (for example obsolete systems) or on the single related events (delays in deliveries, faulty products).

The event identification process results effective when it is able to also identify the existing correlations between various events. By doing so, it is possible to group each potential event in categories both at a business level and operational unit level. Each of these categories is related to a particular business risk category such as: environment risks, process risks, information risks. For instance, environment risks can arise when external forces can affect the company's business model, including all those drivers that lead to the company's objectives achievement. Process risks instead, are concerned with the uncertainty towards the company's business model execution. In particular, this happens when:

- Company's operating processes are not effectively understood, managed, updated, and controlled.
- Company's operating processes are not clearly defined.
- The same processes are not sufficiently aligned with the entity's business model guidelines.
- The operating processes do not satisfy client's requirements or don't generate enough value.

Therefore, all potential events which might have an impact on the business must be identified. The process involves identifying potential events from external or internal sources affecting objectives' achievement. It stands to reason that the management team has to be able to distinguish between events which represent risks and those that represent opportunities in order to assess the risk and take an adequate response.

2.3.4 Risk Assessment

As the word recalls, *Risk assessment*, sets the basis in order to determine how companies' potential risks will be managed. About this, all entities are convicted to face several risks, both internal and external, during their business life. Each of these risks can severely affect the entity's existence. However, there is no way to reduce the risk to zero. Therefore, the management team has the responsibility to set a prudential and acceptable risk level. But what is risk? The word *risk* refers to the possibility that an event occurrence can adversely affect the achievement of entity's objectives. Therefore, the precondition in order to assess all entity's possible risks is the definition of the objectives within the three above mentioned categories: operations, reporting and compliance. Once the objectives have been defined, the management starts identifying and analysing the risks related to those specific objectives through a dynamic and iterative process. The evaluation takes into consideration the probability and the impact of all possible events. Furthermore, the potential's events consequences are analysed throughout the whole entity by taking into consideration both the inherent and the residual risk. The inherent risk can be defined as the risk assumed by the company if it does not change an event's occurrence probability. While the residual risk is defined as the risk that remains within the company even after the risk response implementation. Additionally, the company should be able to subdivide the events into two categories such as possible potential events and unexpected potential events. The firsts comprise all those events which have already occurred in the past, or which occur with a certain frequency. The seconds instead, comprise all those events which are generally not considered within ordinary operating budgets. Another important point concerns the coherence between the time horizon used to assess the risk and the time horizon adopted in the company's strategic planning stage. Furthermore, it would be more appropriate to define the event's impact by using the same measure units as the ones used to quantify the predefined objective's achievement. For instance, to better clarify, if the entity's objective is to increase the quality of its products, then the best unit measure related to the objective will be the number of defective products. Therefore, the company could choose to reduce the defective products by 5%. Accordingly, the impact of the potential risk on the product quality will still be the number of defective products. For instance, the impact related to the risk of incorrect plant setting could cause 9% of defective products. The estimation of probability and impact can be based on historical events or by comparing internal data with the industry's benchmark. Stated this, it is important to dwell on the concept of event probability. About this, the latter can be defined in many different ways according to the event's specific characteristics. Laplace stated in his definition that: "*The probability of an event is the ratio of the number of cases favourable to it, to the number of all cases possible when nothing leads us to expect that any one of these cases should occur more than any other, which renders them, for us, equally possible*". Several other scholars such as Von Mise and De Finetti, Ramsey contributed with their theories. Each of these, considered the event's probability from a different perspective and for such reason all of them are applicable within company's risk assessment process.

To conclude it is important to highlight how the above-mentioned analysis can be carried out for each risk element related to a specific project, a specific business unit rather than to the whole company. All identified risk elements should be synthetized in a matrix in order to view them simultaneously. Therefore, the efficacy of the risk assessment and management processes highly depend on the management team's sensitivity towards risk assessment issues.

2.3.5 Risk Response

The fifth element of the ERM framework is defined as *Risk Response*, which represents the process through which an entity decides how to manage the previously identified risks. In order to engage in risk response, the entity should consider the following aspects:

- How will the responses engrave in terms of risk impact and probability?
- Which response will enable the company to be better align with the identified acceptable risk level?
- What are the related costs and benefits of each response?
- Is there an alternative way for the company to achieve the predefined objectives without having to manage the identified risks?

It is important to underline that risk response generally engraves on other entity's aspects. For such reason, each time, the management team should engage in a systematic reflection in order to consider all possible event's interconnections. For instance, a risk response aimed at reducing the event's probabilities could provide for the introduction of a specific access password in order to prevent resources thefts. Otherwise, the risk response could be aimed at reducing the event's negative impacts by for example introducing an insurance policy to protect the organization from thefts. The choice of the best risk response takes into consideration also past experiences and future forecasts. For what concerns the cost-benefit analysis, which is linked to each risk response, generally companies evaluate the costs that can directly or indirectly be attributed to each possible response. A deeper analysis could also involve the so-called *opportunity cost* which reflects the forgone benefit that would have been derived by a not chosen option. Hence, in this case, the opportunity cost could arise if the company decides to engage in a risk response by employing a resource which could have been used elsewhere. For instance, the management team could decide to reduce the plant breakdown risk by introducing an automated system that is specialised in troubleshooting. Therefore, in this specific case the risk response would lead to the system's expensive purchase and also to other indirect costs. These costs are related to personnel training, supplementary energy and so forth. Of course, each of these resources could be used for other alternative investments and this is what generates the above-mentioned *opportunity cost*. On the other hand, though, the ability to identify potential risk response's benefits is way much complicated. In fact, it is difficult to objectively forecast the positive effects of risks management.

But how does the risk response process work? First of all, risk responses are analysed by members of each company function. The manager of each function provides for an evaluation of the risk and also identifies the residual risk profile, which is the risk that won't be eliminated even after the risk is managed. Secondly, all different evaluations are aggregated, and an overall evaluation takes place. As a third step then, the management team analyses each risk response by posing itself the above-mentioned questions. Once all possible risk responses have been analysed the management team selects the ones that provide for an adequate level of consistency between appetite risk and tolerance risk. If the selected response provides for an excessive residual risk the management team should revise its choices or rather resize the defined risk tolerance level. The following example will help to clarify the risk response process. Consider an entity operating in the industrial sector which has defined its general risk in relation to its gross operating margin. Based on what stated before, each business unit manager identifies the possible risks and evaluates them in terms of probability and impact on the gross operating margin. In order to produce a good analysis, managers usually use graphs as supporting tools. Once all the analysis is submitted, the management team aggregates all information in a unique graph which shows for each business unit the possible events and their possible impact on the company's objective achievement (once again, the gross operating margin). Based on such overall analysis the management team will then decide the most adequate risk responses. It could decide to avoid the risk such as eliminating a certain product, an activity or also its presence in a certain market. It could choose to accept the risk by giving up taking any action. Rather, the team could decide to share the risk, for instance by signing an insurance policy or by signing a hedging contract for the exchange rate risk. Last, but not least it could choose to reduce the risk by acting on the probability or on the impact that this could have. The last two choices are the most interesting ones since they denote the management's will to actively manage the risk and to bring it to an acceptable level.

2.3.6 Control Activities

Control activities are proactively designed to assess and mitigate significant risks. They framework defines them as "*actions established through policies and procedures that help ensure that management's directives to mitigate risk to the achievement of objectives are carried out*". Their main characteristic is that they can be performed all over the entity, at various stages of the business processes and also over the technology environment. They typically range from preventive to detective and can comprise manual or automated activities. As the word recalls, preventive activities aim to deter the instance of errors or frauds. They usually include thorough documentation and authorization practices. On the other hand, instead, detective activities identify undesirable occurrences after the fact. As an example, one of the main activities performed by companies is the reconciliation process. Usually, companies engage in reconciliation when they want to be sure that what they have reported on their accounts matches with what reported in the bank accounts.

Control activities provide for the application of three different principles, such as principle nine, ten and eleven. About this the principles are divided as follows:

1) The entity starts by selecting the control activities that can lead to the mitigation of risks to the achievement of goals to an acceptable level. Once the risks that threaten the achievement of the organization's goals are identified, the responsibility shifts to management teams and BODs. Their job is to define the control activities that can minimize the identified risks and reduce them at least to an acceptable level. For instance, such activities include segregation of duties. By applying this type of control, the management team's aim is to protects itself from the risk that one single person can actually get the control of all the stages of a specific transaction. Also, the company can decide to set authorization limits in order to avoid its exposure to man's fraudulent activities. Of course, such implementations can't totally eradicate the occurrence of fraudulent actions, but they can certainly limit them.
2) The entity relies on technology to put into place the selected control activities in order to support the achievement of objectives. With the introduction of technology many business processes have become automized and computerised. The reason behind this is that technology is known to produce very accurate outputs in a very short time. However, the issued outputs are based on inserted inputs. It stands to reason that, there is an inherent risk of issuing wrong outputs through the presence of errors and misstatements within the inputs. It is clear that even electronic business processes

need to be kept under control. For instance, segregation of duties can be applied in order to avoid one person handling too many processes. In fact, an entity's member could be in charge of handling the input part of a transaction while another one could be in charge of authorizing that specific operation. There are several approaches to implement in order to achieve such principle. For example, companies can configure the IT infrastructure to support restricted access or apply a System Development Life Cycle over Software Developed in House.

3) The entity shares control activities throughout the structure by applying policies and procedures in order to establish what is expected. Even though the previous principles are important, in order for them to be effective they should be properly documented and implemented as policies. Once these policies are finally applied, they can be spread throughout the organization by leaders and managers in various positions

2.3.7 Information and Communication

Starting from the first one, Information is a fundamental element for company's governance. It has been defined as follows: "*Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives*."[17] Despite the way in which it is elaborated (manually or through IT supports), information is the tool through which companies are able to manage and control all business processes. This is why the management team must identify the information needed at each level of the organization in order to fulfil the predefined objectives. In addition, information helps to oversee all external variables that could affect the business reality. Evaluation of management effectiveness and efficiency; reliability of financial statement information and compliance with the law, all rely on the quantity and on the quality of the information issued by the organization. The major problem linked to this type of control lies especially on the quality of information in terms of accuracy, updating, comprehensibility and punctuality. On the other hand, though, also data processing efficiency can represent a weak point for the entity. A fundamental aspect, that should be considered when analysing the information component of internal control, is the timeliness of data provided to people within the entity. In fact, by making a piece of information available with delay can compromise the company's ability to change a certain circumstance. At that point, the data collected would be useless and ineffective. For such reason it is important to timely identify the necessary information and plan the information

[17] COSO, *Internal control-integrated framework*, Executive summary, May 2013.

system by verifying its coherence with the entity's objectives and strategies. Unfortunately, in many countries the information system concept has been combined with the technological one, such that many companies are more concerned with the implementation of the latest technologies rather than with the application of the most adequate information system. It is actually wrong to believe that only the latest technologies can ensure major control and a better data provision. In fact, evidence provided that all small entities which kept the same system, even if outdated, managed to benefit from it. In fact, it turned out that the already existing systems, which have been built and tested considering the companies' specific needs, were way more effective.

Linked to the *information* component there is also *communication,* which can be defined as an intrinsic function of the information system. The 2013 framework defines it as follows: "*Communication is the continual, iterative process of providing, sharing, and obtaining necessary information*." Communication can involve two directions such as communication towards outside and inside parties. For instance, when dealing with the internal context, communication plays an important role since timely communication of quality information enables entity members to perform effectively towards achieving objectives, addressing risks, and supporting the internal control system. Not only, but communication also helps them to understand what the entity expects from each of them. By doing so, entity members will certainly be able to identify not only problems related to their particular activities, but also problems concerning internal controls. For such reason it is extremely important for communication to flow all over the organization and in each direction, such as downwards, upwards, and across the hierarchy. However, also communication towards the external environment plays an important role. In fact, the latter comprises not only information towards shareholders or newspapers, but also information shared with daily third parties such as banks, clients, and suppliers. First of all, the company should understand what it is required to communicate by law (for instance, data breaches or audit reviews) and what instead it would like to communicate with external parties. Companies could be willing to communicate an important organizational change rather than an important acquisition and so forth. Secondly, it is important to have an appropriate channel in order to receive information from external parties. Having a secure information portal could help the entity to share sensitive data with its suppliers, customers, and members.

2.3.8 Monitoring

Through the monitoring activity entities manage to ascertain whether each of the five internal control's components exist and properly function. This is made possible thanks to ongoing or separate evaluations which are proper of all business processes at different levels of the entity, and which provide timely information. While separate evaluations refer to periodic checks, ongoing evaluations are part of routine monitoring activities which are built in the entity's operations. About this the COSO body stated that ongoing evaluations include "*regular management and supervisory activities, peer comparison and trend analysis using external and internal data, reconciliations, and other routine actions*". Furthermore, the framework states that both evaluations can be performed manually or through software's support (automated). Of course, manual processes are physically performed by entity's members, and they provide for the control's evaluation after a certain operation or transaction has occurred. However, using a software as a monitoring tool can help the company to identify and remedy control deficiencies on a timely basis. For instance, a software is able to immediately flag invalid transactions and avoid them to processed further on. This clearly reflects in time saving. Subsequently, findings are evaluated against criteria established by the management teams or by regulators in order to recognise and communicate any encountered deficiency.

Monitoring is also part of the ERM framework since it can be applied also in the risk managing process. Business activity involves the assumption of numerous risks such as assets thefts, environment pollution, personnel's injuries at work and so forth. Hence, risk is a natural element of the business activity, and this is why risk assumption leads to an economic return expectation. It is clear that, over the years, companies are convicted to face different and new arising risks which could modify the entity's level of risk acceptancy. Accordingly, this could affect the entity's risk responses which were once considered effective. This scenario could be determined by several factors, both internal and external. It stands to reason that there are no risk managing tools which are able to keep their efficacy through the years without having to be constantly controlled and revised. Thus, the monitoring process should be able to address the need for revision in the design of control, based on the risk changing. About this, the members involved in the internal control's evaluation process are managers and BODs. They usually select evaluators in order to help them through the monitoring activity. The reason behind this is that these evaluators are also the ones which possess a high baseline understanding of the internal controls and of its related processes. Not only, but they also have authority, resources, and capabilities to perform an internal control assessment. It stands to reason that monitoring can be best achieved when two elements are included. First of all, having a sound "tone at the top" is extremely important in order to ensure employees' positive attitudes towards the monitoring activity. For such reason it is important for managers to walk the walk and not talk the talk. Second, as mentioned previously, there should be an effective organizational structure which is able to assign monitoring roles to people provided of the necessary skills.

2.4 Understanding the importance of ERM'S framework

Clearly risk is totally part of the economic activity, and it is just by taking risks that people base their remunerations or their economic returns. Nowadays companies are operating in an increasingly turbulent, uncertain business landscape where it is always difficult to manage incoming risks. However, companies' survival depends on their ability to generate value for stakeholders. As Meulbroek [18] stated in his book, "*The goal of risk management is not to minimize the total risk faced by a firm per se, but to choose the optimal level of risk to maximize shareholder value*." Therefore, management's challenge is to determine the right level of acceptable uncertainty in order to create value. It is worth highlighting that uncertainty could represent a risk or an opportunity and potentially it could decrease or increase companies' value. Therefore, ERM helps the management team to effectively address uncertainties and the related risks and opportunities. By doing so the system increases the companies' abilities to generate value. To simplify, business risks can be identified in four main categories such as:

- Business risks, related to the company's operating business.
- Market risks, such as price and interest rates fluctuations
- Credit risks
- Operating risks related to the normal business activity.

Failing risk management could be deleterious for a particular company and this is why risk is considered as an important element to consider in the value creation process. This is also the reason why managing risks has become a fundamental step in order for companies to gain success and acquire competitive advantage. Also, the system is quickly ascending to the top of senior's executives' agendas. For what concerns value creation instead, company's actual value can be measured in terms of income-flows generations and prospective cash

[18] L. Meulbroek, *The promise and challenge of integrated risk management* (2002), p. 64

flows generations which are discounted in order to take into consideration the risk associated to the business activity. Therefore, stated this, there are two ways to actually increase the company's value. First, increase the expected flows. Second, reduce the associated risks. Both of them should be pursued simultaneously. Hence, nowadays the main objective is to measure and manage the significant risks in order to mitigate the overall business risk and to optimize the risk-return ratio. However, the problem is represented by today's scenario which is characterised by an unstoppable technological innovation and also by a fierce competition on the capital markets which makes it very difficult for companies to obtain financial resources. Companies which are not able to evaluate and manage business risks can be overwhelmed by this scenario which will negatively impact on their value creation. Hence, ERM is a fundamental approach to manage the organization since it aligns strategy, processes, technology, resources, and skills in order to evaluate and manage risks. This generates also major value for stakeholders since it increases management efficiency. Not only, ERM generates also continued support to the top management together with a clearer and more transparent external and internal communication which increases investors and stakeholder's trust. About this, management maximise value when formulating strategies and objectives in order to achieve an optimal balance between growth and profitability targets and the consequent risks. While in the past internal control systems were focused on some particular risk categories such as financial and assurance risks, today they focus on managing any kind of risk which could compromise company's objectives achievement. It stands to reason that the company's internal control system should be structured in order to guarantee a constant and efficient monitoring of all corporate risks. This will enable the company to maintain its operating conditions. Hence, enterprise risk management ensures company's sound economic, financial and equity conditions. Many sources of information about ERM state that companies should be proactive rather than reactive. This means that by implementing ERM systems companies learn to expect the unexpected. In fact, "*We tend to be overconfident about the accuracy of our forecasts and risk assessments and far too narrow in our assessment of the range of outcomes that may occur.*"[19]

The importance of implementing such system lies on its six unique features:

1) The strategy's alignment to the acceptable risk. The management team sets the acceptable risk level in order to evaluate the possible strategies, set the

[19] Kaplan & Mikes, Harvard Business Review, June 2012

corresponding objectives and develop the tools in order to manage the resulting risks.

2) The Improvement of risk responses. The ERM system provides a rigorous methodology to identify and select among all risk responses the most adequate one (avoid, reduce, share, and accept the risk).
3) The reduction of contingencies and consequent losses. By increasing their ability to identify potential events, evaluate the related risks and give adequate risk responses companies reduce the frequency of unexpected events so as the consequent costs and losses.
4) Correlated and multiple risks' identification and management. Each entity has to face several risks related to different business units and ERM facilitates the formulation of an effective risk response with correlated impacts and unique responses to multiple risks.
5) Opportunities identification. By analyzing all potential events, the management team can identify and proactively understand the emerging opportunities.
6) Improving capital use. The acquisition of risks' reliable information enables the management team to effectively assess the overall financial needs and to improve capital allocation.

These six features are proper of the ERM system, and they help the management team to achieve their performance and profitability objectives and also to avoid resources losses. In addition, they help to ensure the effectiveness of reporting and compliance with laws and regulations and to avoid damages to the corporate image. In summary, ERM supports the organization in achieving the desired goals, avoiding pitfalls and unexpected events.

However, in order for the model to be effective each body within the company should act as follows:

- Board of Directors. The board must discuss with the top management on the status of the corporate risk management process and if necessary, it should supervise the process itself. The Board must be sure to be well informed about the most relevant risks and the related management actions. Not only, it should be aware of how the management is operating in order to make the system effective. The board can also obtain information related to this purpose, by contacting internal or external auditors and so forth.

- The CEO should assess the adequacy of the risk management process adopted by his entity. A possible approach could be a meeting with leaders of operational units and personnel responsible of key tasks in order to prepare a preliminary assessment of the adequacy and effectiveness of the process in place. Despite the form, a preliminary evaluation will have to establish whether there is the need to engage in a subsequent broader assessment and how to do it.
- Other personnel. Managers and other personnel of the structure will have to make sure that their responsibilities are materialised within the company's reality and study the proposals which could strengthen the risk management process.

To conclude, a good and sound ERM helps companies to obtain capital access which in turn enables them to implement their strategies and increase investments' values. In fact, academics have found that ERM adds value to firms thanks to its ability to create economies of scales, synergies through information sharing, as well as balancing risks that reduce the total risk management costs.

3 Chapter 3 - Evidence for Fraud: The WorldCom scam

In 2002 WorldCom, U.S. second largest long-distance telecommunication company, announced that it had overstated earnings in 2001 and also during the first quarter of 2002, by more than $3.8 billion dollars through the use of improper accounting methods. It was appointed as the largest accounting failure in the United States' history. But how could a loss of such magnitude have occurred?

To answer this question, it is necessary to introduce several interrelated concepts such as the context in which the company was operating, the role of Internal Auditors at WorldCom and their relationship with the ERM framework which, in turn, is linked to the giant's internal control system. Each of these aspects has been fundamental in the fraud occurrence and only a deep analysis of the dynamics that link such elements can provide an understanding of how the fraud scam really evolved.

In order to better appreciate the topics introduced in the first part of the paper, the following chapter will focus on WorldCom's fraud case. In fact, the latter represents a concrete example of a financial statement fraud which occurred with the presence of three Fraud Triangle's elements: Pressure, Opportunity, and Rationalization. It is also a perfect representation of how the lack of internal controls, which has often been reported by the company's Internal Audit department, and the Corporate Governance failure, have been the key drivers of this important fraud scheme. Not to mention how the fact helped to inspire what is now known as the ERM framework, which has been designed in order to help organizations to deal with risks that have increased in volatility and complexity as they face increased regulatory pressure.

3.1 Background on the case

Born from the idea of two local entrepreneurs, William Rector and Murray Waldron, LDDS (Long Distance Discount Company) started its business activity in Mississippi, the hub city with an easy access to the major cities Jackson and Orlando, in 1983. The small company was the official predecessor to WorldCom. During the 90s, from a small Mississippi provider of Long-Distance telephone services, the company started acquiring several other telecommunication firms which helped it boost its revenues up to $39.2 billion in 2001. It provided a broad range of communication services to consumers and businesses in more than 65 countries. It was Bernie Ebbers (CEO) primary strategy, achieving impressive growth through acquisitions such that in less than twenty years he managed to lead the company through seventy acquisitions. Surprisingly in 1989 the company became public with the acquisition of Advantage Companies Inc. This bold spirit led Bernie Ebbers to acquire the name of "Telecom Cowboy" and to be recognised as the man *Business Week.* About this, some acquisitions involved UUNet, Williams Technology group, IDB communications group, but the most important one has been Advanced Telecommunication Corporation's acquisition (ATC) in 1992 which made LDDS the Nation's fourth largest long-distance company. In fact, at that time the competing environment was dominated by three big rivals such as AT&T, Sprint, and MCI. It was just with the takeover of the latter, in 1998, that WorldCom become the second largest U.S. long distance carrier, known as MCI WorldCom. The company in fact was two and a half times WorldCom in terms of revenues. In 1999 MCI WorldCom and Sprint announced their plan to merge. However, both the European Union and the United States department opposed to the proposal. In fact, had the merger occurred, WorldCom would have gained the monopoly of the long-distance telecommunication sector. Of course, this raised deep objections by the Antitrust commission.

Despite the great number of acquisitions, it is important to focus on the way in which CEO Bernie Ebbers projected to pay for this acquisition binge. In fact, to accomplish the buying of firms he relied on WorldCom's stocks, which meant that there was a great pressure to keep stock price high. Therefore, the board was assembled with executives who gained WorldCom's stocks for their companies, thus leading the board members to have significant assets tied up in the company stock. This was the main reason why WorldCom's executive team was always focused on stock price, on next acquisitions and most important thing, to meet Wall Street's expectations. Given this initial background it is worth analysing each key driver in order to understand how the interrelation of each element contributed to the occurrence of one of the largest accounting frauds in history.

3.2 Understanding the fraud scheme

In the precise moment in which WorldCom reported that it would have restated the $3.8 billion of operating expenses which it had improperly capitalised, its stock price had already fallen from a maximum of $64 in June 1999 to a minimum of 83 cents. Furthermore, in April 2002, two important rating Agencies, S&P and Moody's, cut WorldCom's long-term and short-term ratings to junk. To appreciate what caused such a failure it is necessary to understand the impact of executives' decision making as well as the lack of integration within the company. Also, great importance should be given to the external factors that came into play.

- External Factors

The context in which WorldCom operated represents one of the main reasons of its failure. In fact, in the 90s the industry was particularly focused on internet expansion and on building the infrastructures to support it. This optimism towards internet growth led many companies, even very small entities, to enter the telecommunication market with the aim of making profits. However, when barriers to entry are particularly low the immediate consequences are oversupply and hyper competition. This was exactly what happened to the telecommunication industry in that period. The industry was totally overestimated, there was great confidence on companies' potentials, and great deregulation of the telecom industry. This led to an exponential increase of companies' stock price. Despite the tremendous speculation, there was also a massive borrowing by Dot.com companies taking advantage of low interest rates. In fact, in that period the Federal Reserve system (FED) did not take any action in order to avoid the bubble burst. On the contrary, it continued to lower interest rates until June 1999. Peter Hartcher, a financial journalist of that time, stated in one of his books (Bubbleman) that "*The Fed, in short, was feeding cheap money into the bubble*". Therefore, in 2000 the combination of market saturation and companies' revenues which fell short of expectations, led investors to divest before securities could be further depreciated. The bubble burst took down many of WorldCom's biggest customers such that in 2000 the industry slowed down, and the company found itself in heavy debt and with great difficulties in generating revenues. In fact, in that period Dot.com, web hosting and new telecommunication companies started cancelling orders for fiber-optic capacity leading suppliers such as WorldCom to fall. Just to have an idea, the market value of WorldCom's common stocks went from $150 billion in January 2000 to less than $150 million in 2002. Clearly, the desire to avoid such a stock market loss represented a great incentive for executives to indulge in illicit actions.

- The Accounting Manipulation

In October 2000, David Myers, WorldCom's controller, was shocked by the amount of costs emerged during the closing of the books for the third quarter. Inexplicably, the line cost expense, which represented the costs incurred by the company to lease telecommunication lines, was high by hundreds of millions of dollars, which meant that revenues would have failed to meet Wall Street's expectations.

To clarify, Line costs were WorldCom's major operating expense reported on the Income Statement. They represented fees paid to third parties to access their network facilities. In fact, in 1990 WorldCom signed a great number of long-term leases to have access to third parties' networks. By signing those contracts, WorldCom was supposed to pay the third party a fix sum throughout the whole term of the lease regardless of whether the company actually used all the facilities. Under the GAAP (Generally Accepted Accounting Principles) these costs must be recorded as expenses on the company's Income Statement. For instance, when a WorldCom customer made a call from New York to Italy the call would first pass through New York's local phone company and then through WorldCom's long-distance line towards Italy.

Considering the company's poor results, the very first conclusion was that certainly someone must have made an error. However, by going through the numbers again, no mathematical mistake was found. In fact, around July 2000 the company's expenses, as a percentage of the total revenues, exponentially increased, thus leading to a decline of WorldCom's income. Therefore, David Myers had no other choice but to present his findings to Scott Sullivan, who at the time was WorldCom's CFO. To make things worse, soon the company had to release its financial results to the public. Showing such poor results would have undermined the stock price and analysts would have downgraded their opinion, thus leading investors to divest their money.

This scenario created great pressure among WorldCom's executives such that in order to meet market's expectations and to continue to rely on stock price to acquire companies, CFO Scott Sullivan ordered David Myers to reduce line cost expenses. However, considering their roles within the company neither Sullivan nor Myers could actually have access to the company's accounting entries' system. For such reason they decided to involve two mid-level accountants in order to change and adjust financial results. As the following chapter will show, both accountants were extremely uncomfortable with the Controller's request, but in order to keep their job they decided to get along with the plan.

It is worth mentioning that all the opinions expressed on Telecommunication companies were usually based on the E/R ratio which is a critical performance indicator focused on the relation between line-cost expenditure and revenue. Considering that WorldCom's E/R ratio amounted to just 42% (far below competitor's ratio) there was great pressure to increase the appearance of revenue growth while reducing costs. The numerator of the ratio was represented by WorldCom's line costs expenses which involved all payments incurred to lease phone network lines. For instance, WorldCom's closest competitors reported 46.8% and 53.2% as E/R ratio. This should have represented a red flag from the beginning.

Stated this, as its common knowledge, accounting is made of estimates, especially when dealing with acquisitions. Companies make estimates on the liabilities and expenses that they will incur. However, sometimes these financial statement lines are overstated. This does not represent a problem if once the exact number is determined the estimation is corrected. But, as the first chapter highlighted, many companies choose to leave the numbers as they are creating the so called "Cookie-jar reserves". These are savings that companies illicitly use to cover future poor results. For instance, companies might set reserves to cover litigation, bad debts or also job cuts and acquisitions. By drawing down these reserves WorldCom's mid-level accountants tried to reduce the E/R numerator. However, there was no justified reason or proper basis to reduce such amounts. First of all, accruals were released without the support of an appropriate analysis to understand whether the company was actually having an excess number of accruals or not. Secondly, even when WorldCom had an excess number of accruals, these were released in improper periods to cover poor results. About this, according to GAAP, accruals should be released only in the period in which they have been identified and not later on just to improve the company's results. Third, WorldCom released accruals that did not refer to line costs expenses rather they had been established for other purposes. This method of reversing expenses inflated earnings, thus leading the company to meet market expectations. However, these manipulations deliberately misled and defrauded investors, also considering that behind there was no legitimate business rational and no supporting documentation to reverse such expenses. By doing so between 1999 and 2000 WorldCom managed to reduce the reported line costs by approximately $3.3 billion. Both Myers and Sullivan promised to reduce earning guidance in the next period such that the false entries were just a one-time thing. This was not the case though.

Again, when closing the financial statements in the fourth quarter the accountants discovered that earnings were still below expectations and despite the new lower guidance they were still not enough. This time the problem was serious thing. In fact, the "Cookie-jar reserves" were totally depleted, there was no excess amount to draw down. Therefore, Scott

Sullivan proposed to indulge in a new fraud scheme, which provided for the classification of line costs as capital assets.

The reason behind this choice is related to the existence of a different accounting treatment between costs of capital assets and operational expenses. The firsts can be written off over longer periods while the seconds must be exclusively recognised in the period in which they are incurred. In fact, operational expenses comprise all expenses incurred by the company during its normal operations, for instance salaries and wages, electricity and so forth. On the other hand, capital expenditures result in acquisitions or improvements to company's assets, for instance computer equipment, real estate and so forth. Generally, operational expenses are reported in the company's Income Statement and subtracted from revenues, resulting in company's net income. Capital expenditure, by contrast, are recorded in the Balance Sheet as capital assets. Therefore, by treating operational expenses as capital assets' costs, Scott Sullivan's aim was to spread expenses over longer periods by increasing its current net income and its assets (since capitalised costs were treated as investments). As the SEC investigation report stated, from the first quarter of 2001 up to the first quarter of 2002, WorldCom managed to reduce line costs by $3.8 billion, by capitalizing line costs for $3.5 billion.

To have an idea, the consequences of WorldCom's fraudulent accounting schemes on the forms filed with the Commission can be summarised in figure 8 below. As the table shows, there are two types of forms that companies must submit: the 10-Q form and the 10-K form. The first is a quarterly mandatory report required by the Security Exchange Commission (SEC) which contains entities' financial performance, internal controls, management discussions and disclosures. The second instead, is an annual report that offers a comprehensive summary of entities' financial performances which includes information such as the company's history, its organizational structure, its equity, its audited financial statements and so forth. For instance, in the second quarter of 2001 WorldCom reported $159 million of net income while, in the same period, the company was actually experiencing a loss of $401 million. Furthermore, each of these forms failed to include the "new" and illicit accounting treatment used to classify operating line expenses. The company should have disclosed that the operating expenses were actually increasing as a percentage of the total amount of revenues and that the treatment of such expenses had changed with respect to the previous periods.

Form filed with the Commission	Reported Line costs Expenses	Reported Income (before Taxes and Minority Interests)	Actual Line costs Expenses	Actual Income (before Taxes and Minority Interests)
10-Q, 3rd Q. 2000	$3.867 billion	$1.736 billion	$4.695 billion	$908 million
10-K, 2000	$15.462 billion	$7.568 billion	$16.697 billion	$6.333 billion
10-Q, 1st Q. 2001	$4.108 billion	$988 million	$4.879 billion	$217 million
10-Q, 2nd Q. 2001	$3.73 billion	$159 million	$4.29 billion	$401 million **loss**
10-Q, 3rd Q. 2001	$3.745 billion	$845 million	$4.488 billion	$102 million
10-K, 2001	$14.739 billion	$2.393 billion	$17.754 billion	$622 million **loss**
10-Q, 1st Q. 2002	$3.479 billion	$240 million	$4.297 billion	$578 million **loss**

Figure 8."WorldCom's false statements in Filings with the Commission"(Source SEC Report of Investigation, March 31, 2003)

By the way, Misclassification was just one of the various techniques used to cover the financial fraud. For instance, the merge in 1998 with MCI company represented another great opportunity to defer costs. This time though, WorldCom focused on the figure of Goodwill. To give a clear representation, Goodwill is the difference between the actual purchase price paid to acquire an entity and the net book value of its assets. Therefore, it is considered as the excess purchase price, and it is classified as an intangible asset. As the first chapter showed, intangible assets are depreciated over their estimated useful life. In this case though, Goodwill's depreciation is based on the estimation of the respective asset's useful life. The plan was to reduce MCI's assets net book value to generate a higher goodwill to depreciate over the years. In fact, at that time the GAAP (Generally Accepted Accounting Principles) permitted Goodwill's amortization over 40 years which enabled WorldCom to show very small amounts of expenses each year.

Along with cost capitalization and improper accrual release, WorldCom continued to disclose impressive revenue growth numbers even when its competitors where being hardly hit and affected by industry trends. The reason was that starting from 1999, WorldCom's personnel started booking higher revenues after every quarter closing. By doing so, they managed to show CEO Bernie Ebbers that the company was achieving the revenue targets that he had established. In fact, everybody was aware of how Bernie Ebbers was intensely focused on revenue performance and how he closely examined the Monthly Revenue report. Therefore, members of the accounting department, directed by CFO Scott Sullivan, started calculating the difference between actual revenues and projected ones. In order to meet target revenues, they started booking entries to make up the difference. However, these entries could not figure as revenues from operating activities, or they would have masked real numbers. For such reason they were recorder in a separate account defined as "Corporate Unallocated" which was reported as a separate section in the Monthly Revenue report. As previously stated though, just few people could have access to the Monthly Revenue report. The interesting thing about these entries was that they used to appear just in the quarter-ending months while there was no trace of them during the entire quarter. To have an idea of the numbers reported, the highest amounts of revenues ranged from \$136 million to \$257 million. In particular, booked revenues were associated with "Minimum Deficiency charges" that derived from customer's billing when their usage amount was below the minimum one established by contract. In fact, customers who entered a contract with WorldCom were supposed to use a minimum number of minutes in order to obtain an advantageous price. However, if customers under-utilized the minimum usage the company would have been allowed to retroactively bill the customer. Collectability of such amounts could take place only if they were established with reasonable assurance or else GAAP would not allow for revenue recognition to take place. Clearly, without inflating revenues WorldCom would have failed precisely in six out of twelve quarters, considering the period going from 1999 to 2001.

In general, perpetrators manipulated the financial results in two main ways. First of all, in 1999 and 2000, they reduced operational expenses by improperly drawing company's reserves, known as "Cookie jar reserves". Secondly in 2001 and early 2002, they improperly represented operational expenses as capital assets. Neither of the two methods complied with the GAAP (General Accepted Accounting Principles) and neither of the two methods was disclosed to investors even if they represented a change in the previous accounting treatment. However, both methods contributed to decrease WorldCom's expenses while artificially increasing its financial statement's revenues from 1999 to the first quarter of 2002. Evidence of the number of improper adjustments to line costs by quarter is presented in the following table.

Improper Adjustments to Line Costs
(in millions of dollars)

1Q99	2Q99	3Q99	4Q99	1Q00	2Q00	3Q00	4Q00	1Q01	2Q01	3Q01	4Q01	1Q02	Total
(41)	103	140	396	493	683	832	862	771	606	744	942	798	**7.392**

Figure 9."Improper Adjustments to Line Costs" (Source SEC Report of Investigation, March 31, 2003)

- Failure of the External Audit Firm

To make things even worse, WorldCom's management team acted in order to keep the external audit firm, Arthur Anderson, from finding the ledger entries. About this, Arthur Anderson has audited the company from 1990 to 2002 and it had always considered WorldCom as its "Crown Jewel". However, the audit company was totally aware of the "high risk" that WorldCom represented, mainly due to its business activity. The first problem was represented by the high volatility of the telecom sector which has been classified as a red flag, a potential threat for the external audit company. The second reason was represented by WorldCom's aggressive strategy, which included all acquisition and merger plans and its reliance on the stock prices in order to acquire target companies. All these elements should have brought Arthur Anderson to refuse the assignment to be WorldCom's external auditor. However, considering that the company represented a highly coveted client, the external audit firm decided to rate WorldCom as "moderate risk" and keep its long-term partnership with the company.

To keep the Audit firm from finding the improper accounting entries, WorldCom's executives plan was to ask the audit firm to direct all the requests through a single person. By doing so, WorldCom was sure that nobody else, except the one responsible of the account's manipulation, could directly interact with the audit firm. Furthermore, Arthur Anderson did not have real-time access to WorldCom's accounting system. Despite several requests, the firm could not access the system to search any non-routine entries. Arthur Andersons seemed to have no control over the audited company, its way of acting never led to any change. Anderson's audit approach had several apparent flaws. For instance, in August 2001, one of Arthur Anderson's partners wrote an email outlining all the planed testing procedures and sent it to WorldCom's accounting management. The e-mail was sent unintentionally, but this gave fraud perpetrators enough time to cover up the fraud and move the amounts out of the accounts that the audit firm wanted to test.

Early in 2002, Cynthia Cooper, head of the Internal Audit department, was asked by a colleague to investigate some unusual accounting entries at WorldCom. In order to better understand the situation, she approached a partner at Arthur Anderson to discuss the matter. However, the partner did not seem worried, and he assured that everything was under control such that company's allowances were totally adequate. This was not the case though. Cynthia Cooper went over the company's financial statements and traced all the entries that had been reversed through the system. The next thing she did was to inform the SEC (Security Exchange Commission) responsible of enforcing securities laws in the US.

3.3 WorldCom under a COSO evaluation

The importance of the COSO framework has been deeply analysed in the second chapter of the paper. As the chapter highlighted, the five COSO elements such as Control Environment, Control Activities, Risk Assessment, Information and Communication, and Monitoring, are fundamental criteria in order to evaluate the potential effectiveness of any internal control system and to understand its vulnerability to fraud. They are also helpful to give a backward look to fraud cases and to explain how they have occurred. By using the lessons learned, it is possible to avoid or detect unexpected behaviours, potential mismanagement, and also probable frauds. Of course, compliance can be challenging and expensive, but not as costly as recovering from fraud. This is why it is interesting to look at WorldCom's scam under a COSO magnifier.

By analysing each component of the framework, it is possible to point out all the weaknesses of WorldCom's internal control system which have been the main drivers to financial fraud. In fact, the internal control system should be the basis of a company's development plan. It is part of the management process and if not properly implemented it could cause serious problems to companies.

Unfortunately, at WorldCom the internal control structure was totally inefficient. Starting from the Control Environment where managers never established a culture of ethical behaviour nor strong systems of values such as codes of conduct. Furthermore, there was no sign of employee training and development or executives leading by example. All these measures totally lacked. Of course, when the CEO believes that implementing internal controls is just a waste of time and money, results cannot be different. As the following chapter will show, several times Cynthia Cooper (head of the Internal Audit department) tried to educate the management team on the importance of internal controls by reporting some inefficiencies that she had spotted within the organization. However, when the only objective was to be the n°1 stock on Wall Street the rest takes a back seat.

Within WorldCom, the role and the advice of the Internal Audit department were totally underestimated such that Cynthia Cooper started her journey in the company with just two colleagues who lacked proper experience and training to complete testing. Furthermore, they were provided with a limited access to the company's financial statements and for such reason the internal audit department had just a partial picture of the company's financial statement situation. It is important to underline how Internal Audit is the body in charge of "monitoring" the implementation and the effective operation of controls. It also assures the Board of Directors that risks have been properly identified and reported. The turning point is that they should provide an "independent" assurance. In fact, Independence is at the basis of the COSO framework. However, the reporting structure lacked the independence requirement. As the following section will show, the Internal Audit department reported issues to the same person in charge of audited departments, Mike Cipicchio. The following chapter will provide for the analysis of the causes that led to the biggest US financial scam under each of the five COSO framework's components.

3.3.1 Control Activities

As stated in the second chapter, Control Activities represent a fundamental element within an organization. They embody actions established by procedures and policies to help management mitigate risks in the objective achievement. About this, a big problem within WorldCom was represented by Internal Auditor's preliminary findings. Regularly the Internal Audit department had to prepare a report to summarize company's inefficiencies and to point out any area of improvement. This should have been useful to managers in order to understand in which areas to focus their attention. However, in the company's existence, nor the Audit Committee neither the management team had ever seen such a detailed Internal Audit report. In fact, all the reports issued by the department highlighted how, as a natural consequence of acquiring so many companies, the giant's structure was too decentralized, full of redundant operations and with very poor internal controls. Not to mention that too many employees could easily change billing rates and issue credits, or that sales employees could manually calculate commissions themselves, which clearly meant that no segregation of duties was actually being respected. In fact, within each company there are four critical activities which should be separated in order to avoid fraud:

- Authorizing events (e.g., approving a shipping to a customer)
- Recording events (recording transactions into the general ledger)
- Custody (e.g., keeping the inventory in a store)
- Overseeing (e.g., board of director's review).

This separation seems a very simple process, but it is necessary to ensure that no employee can actually pursue similar activities or seeing through all the stages of transactions without having an independent review. If not properly followed and verified, it could lead to disastrous consequences. Considering its importance, Segregation of duty is typically built in the development and selection of Control activities. However, within WorldCom, the lack of such segregation led to the manipulation of financial information.

Again, related to the selection of control activities that could mitigate risks, WorldCom sales employees were found to calculate commissions manually on spreadsheets. Of course, this way of operating increased the possibility of committing errors and also fraud while it minimised any chance of fraud detection. Therefore, no one from the management team ever tried to establish control activities in order to eliminate risks or reduce them to an acceptable level. For instance, during one of her scores of recommendations, Cynthia Cooper proposed the introduction of automate commission calculation to improve efficiency and effectiveness of operations.

For what concerns financial data, controls over financial information was totally unreliable. In fact, CEO Bernie Ebbers just wanted to hit the numbers by being the N°1 stock in Wall Street, while CFO Scott Sullivan was not able to accept financial reporting when numbers did not match what he had expected. Regardless of this, the company also lacked an Internal handbook for accounting which could have helped to handle complex accounting situations. Probably such a measure, which however would not have been an absolute control, would have helped to limit the potential degree of the financial damage.

3.3.2 Monitoring

As the third line of defence of the organizational framework, Internal Audit provides "reassurance" to the Board of Directors that: risks have been effectively identified and evaluated, that the risk management process is effective and efficient and that key risks have been appropriately reviewed and reported to those who should know. Internal Auditors are the ones performing the "monitoring control" identified within the COSO framework. Therefore, while external auditors have a more focused mandate (they audit companies' financial statement to ensure compliance with accounting principles), Internal auditors have a broader range of tasks which include operational audits (internal controls review, effectiveness, and efficiency of procedures review) and system audits (for instance, verifying that access to critical system data is under control). It is clear that in defining the Internal Auditor's role the recurring words are *risk* and *internal control*. About this, there is a direct relationship between the three. In fact, Internal Auditors might undertake some consulting roles within the ERM framework, for instance:

- Supporting managers in risk identification and help them to find the best solution to mitigate risks.
- Introduce the ERM framework in order to leverage its expertise in control and also risk management.
- Provide advice and coach the organization on risk and control.

Therefore, stated that Internal Auditors may extend their involvement in the ERM's framework, it is also important to highlight that some conditions must necessarily be met. In fact, Internal Auditors cannot replace the executive team in the risk management process, neither they should manage risk on behalf of the management team. Also, they are not supposed to take any decision related to risk management, they should act as a mere supporting and consulting team. However, as explained in the previous chapters, one of the elements which acts as an integrated part of the ERM's framework is "control". In fact, it is not a surprise that the *control environment* element is set as the first component of the IC-IF revised in 2013 by the COSO body. The framework's component is supported by some of the most important principles:

- The organisation demonstrates a commitment to integrity and ethical values.
- The BOD demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of its objectives.

In light of this specific background, how was WorldCom's Internal Auditors role perceived within the firm?

The main problem which seemed to recur during the entire WorldCom's business activity was the poor consideration towards the Internal Auditor's department. Several time Cynthia Cooper (Vice-president at WorldCom's Internal Audit) alerted the Committee that she urgently needed other auditors to help with the great load of work. Despite the countless requests, she has never been considered. The department was totally understaffed. As Cynthia reported in her book: "*I took a risk by going to work for WorldCom-then known as LDDS (Long Distance Discount Services)- establishing a start-up Internal Audit group with only two staff auditors; both of whom had virtually no prior audit experience*."[20]

[20] Cooper C., *The journey of a corporate Whistle-blower*, p.363, 2007

Other reported problems concerned customer call centres which had very long holding times, high number of unanswered calls and very poor call-centre objectives and metrics to be able to monitor the performance. Therefore, in light of what previously said, Internal Auditors should have supported and advice management teams. This was what Cynthia Cooper's team actually did. They provided scores of recommendations in order to improve internal controls and also the efficiency and efficacy of operations. Also, they proposed several changes within the company's organizational structure such as the replacement of manual calculation with automated ones in order to decrease risks of errors or fraud, restrict the system access and the consolidation of costumer's call centres. The reason behind this poor organization was that WorldCom has always been better in acquiring rather than integrating. In fact, each time, there was another acquisition in the horizon, such that integration was delayed with the hope that the next target company might had superior systems.

However, none of the above-mentioned proposals was actually considered since CEO Bernie Ebbers was very reluctant towards internal controls and standardised policies and procedures, which definitely shows how principle number one has totally been compromised. In one of her several interviews Cynthia Cooper stated that "*My team and I had to educate management on the importance of implementing internal controls and developing a strong internal audit function. Bernie Ebbers, the CEO, didn't start his career in business. He had a degree in physical education. He simply hadn't been exposed to internal audit or the concept of internal controls. At one point in the early years of my career, I was told by my boss not to use the term "internal controls in any more audit reports because Bernie didn't understand what it meant, and it aggravated him. Of course, we continued to use the term "internal controls" and instead worked to educate Bernie on why controls were important.*".[21] Certainly, Bernie Ebbers' higher priorities were not codes of conducts and integrity rather his interest was directed to upcoming deals, stock prices and next acquisition targets such that improving internal controls was perceived as a total waste of money and time. Therefore, while sound companies periodically organize Audit Committees meetings to keep updated on the last findings and improve the company's situation, Bernie Ebbers attended just one meeting which proved his overwhelming interest towards internal controls. As mentioned in the previous chapters, Codes of conducts are fundamental in order to establish roles and duties of each corporate office as well as the company's principles. In WorldCom,

[21] Carozza D., *Extraordinary Circumstances-An interview with Cynthia Cooper*, Fraud Magazine, March 2008

this need was even more relevant considering its presence in the multinational territory with several detached headquarters.

3.3.3 Control Environment

The *Control Environment* emphasizes the importance of integrity and ethical values. However, as reported by Cynthia Cooper in her book and also in many of her interviews, within WorldCom there was an "individualistic Culture" where loyalty to the company was less appreciated than loyalty to people. For instance, the two mid-level accountant who were forced to manipulate the accounts were totally respected by CFO Scott Sullivan and Controller David Myers. Furthermore, the only tone at the top perceived was that no one had to question the choices made by the top boss, nor the plans nor the actions. It stands to reason that, with such an embedded culture, all employees felt that they did not have any right to express their opinion or concern regarding the company's behaviour and policies. To make things worse, due to the great number of acquisitions, WorldCom did not have an integrated structure, and this generated great confusion among employees on who to report any type of concern. For instance, the company had eleven separate customer-service centres and three payment-processing departments. While the company's headquarters were in Mississippi, the accounting department was in Texas, the Human Resource in Florida, while the Law department in D.C. Clearly this geographical allocation represented a disadvantage for employees who wanted to raise any concern. About this Cynthia Cooper reported in her book: "*As each company acquired comes into the fold, there is a clash of cultures, political jockeying, management turnover, and reorganization. And key executives are scattered: Boca Raton, Florida (head of Human resources); Washington, DC (Chief legal counsel); Dallas, Texas (Chief operating officer); Clinton, Mississippi (head of commercial sales)*."[22]

As the third principle of the IC-IF states, the management team, with the oversight of the BOD, should establish the structure and the reporting lines in order to pursue the company's objectives. However, this was not what happened within WorldCom. The independence of the reporting structure was totally compromised. Initially, the Internal Auditors department had to report to Mike Cipicchio, who was also in charge of managing Payroll, Account's payables, and Commission's departments. Clearly, all those departments were object of examination by Internal Auditors. It stands to reason that, reporting problems related to

[22] Cooper C., *The journey of a corporate Whistle-blower*, p.190, 2007

such areas to the same person who was in charge of them, totally compromised the independence of the reporting structure. On the contrary, the internal Audit department should have reported to the CFO (Scott Sullivan) and functionally to the Audit Committee. By doing so the CFO would have handled all the administrative functions such as promotions and salaries, while the Audit Committee would have provided some independence from the management team by approving the audit plan. However, elevating the reporting structure was not one of WorldCom's first priorities.

WorldCom also lacked a Nomination committee which is usually responsible for recruiting best qualified candidates. In fact, members of the Board of Directors were personally appointed by CEO Bernie Ebbers. For instance, during an attempt to improve economies of scales by approaching TMC's (Telemarketing Communication of Mississippi) franchise owners, Ebbers decides to offer John Porter, an Atlanta-based entrepreneur, the position of Chairman of the Board in order to convince him to sell the company. This type of behaviour was recurrent, he often offered the Chairman's position and Board seats as a leverage to persuade top decision-makers at the companies he decided to acquire. Additionally, he made sure to personally appoint the majority of the board seats members even when this was not in the company's best long-term interest.

In the period between 1999 and 2002 the Board of Directors at WorldCom was made up of more than 50% of non-executive members. They were mainly members or directors of companies acquired by WorldCom. This type of relationship, other than independent, led the Board to blindly trust the management team's decisions and permitted the management team to have complete control over the Board's agenda. As the investigative committee reported, the Board was not very involved with the company's working. For instance, it never established processes that could encouraged employees to contact external parties about any concern or operational matter. What the Board did was to set a bonus plan to reward short-term revenue growth indirectly creating an incentive for managers to indulge into illicit behaviour. Furthermore, the only time the Board took an active role was in November 2000 when CEO Bernie Ebbers asked the board to grant him low interest loans to pay off his personal debts. About this, besides being CEO at WorldCom, Bernie Ebbers was personally involved in other businesses which included real estate ventures, hotels, country club and a luxury yacht building company. In order to finance such businesses Ebbers relied on bank's loans which he secured with its personal WorldCom's stocks. In November 2000, the Board finally decided to stop Ebbers from selling its WorldCom stocks to repay his debts. However, that was the only time the Board actually played an active role.

As stated in the second paragraph of the paper when dealing with the ERM framework, the Board of Directors has a very important role within the company. In fact, the body has the responsibility to adopt a system which is adequate to the company's characteristics. Not only, it should discuss with the top management on the status of the corporate risk management process and if necessary, it should supervise the process itself. The Board must be sure to be well informed about the most relevant risks and the related management actions. Furthermore, it should be aware of how the management is operating in order to make the system effective. However, at WorldCom no Board member really cared about WorldCom's working, people were just interested in possessing company's stocks which made the Board passive and ineffective. In her book Cynthia Cooper describes the relationship between Bernie Ebbers and the Board members and she reported that: "*It usually took about a year or more to come together. But after a while, as the board members began to make money in their stock, they decided they liked Bernie, and they became us."*.

3.3.4 Risk Assessment

As mentioned in the second chapter, risk assessment is important to assess the magnitude and the size of company's risks. By doing so, the management team has the possibility to focus its attention on the most important threats and opportunities and to prepare a sound risk response. Within WorldCom risk assessment has always been undervalued. For instance, CEO Bernie Ebbers had a wrong risk prioritization. He was always obsessed by holding down expenses, complaining also about travel costs. About this, CFO Scott Sullivan once stated that the CEO was concerned about employees driving seven hours of trips instead of flying because it boosted the company's costs. Similarly, he cancelled the free coffee policy in order to save $4 million. However, what he should have seen instead was the existence of threatening risks such as the under-use of telecommunication lines which represented the main reason to indulge into accounting manipulation. About this, in her book "Extraordinary Circumstances: The journey of a Corporate Whistle-blower" Cynthia Cooper reported Charles' words on CEO Bernie Ebbers. Charles was Cynthia Cooper's boss during her final year at WorldCom. He was the one reporting directly to Bernie Ebbers. "*Bernie only focused on what he liked and understood.. He would focus on someone spending $900 instead of $600 on a plane ticket. But I could never get him to look at a capital budget for billions of dollars. He didn't want to understand the details of building networks or capital plans* *because it was too complex*"[23]. This is the reason why risk prioritization totally lacked since priority was given to travelling costs or other minimal expenses.

As stated in the second chapter, risks exist at all stages of a business cycle. However, in good times, many companies tend to become more relaxed on the potential risks that they could incur. This is mainly due to an increase of confidence and to the increasing euphoria due to easy money making. Both lead to an abandonment of risk management. Besides, in a big company such as WorldCom, that has gone through seventy acquisitions in more than sixty-five countries, the Board and the management team should have given the right importance to risk assessment procedures. However, as the accounting and financial systems became more complex the Board of Directors became totally absent and detached from the supervising of risk assessment procedures. For instance, with a speed of approximately 10 acquisitions per year, WorldCom's risk posture became more and more complicated. While the company was growing, also its debt burden was expanding up to the point that the Board failed to analyse how the debt would have been carried and then retired by the company. This of course contributed to increase the liquidity risk of the entity. Not to mention how the rapid acquisition of other telecommunication companies led to a failure of systems integrations, network integrations, commission plans. All this led to an increase of the control risk within WorldCom. As reported in Thomas Clarke's book: *"Internet planning in particular has failed to address cost issues or the possibility of slower than expected growth, though the company was betting tens of millions in investments predicated on executives' wild guesses about internet growth. Though wireless substitution was then and is today one of the most serious risks for WorldCom, even this was not the subject of serious analysis by the board..The board failed to understand WorldCom's risks-including Ebbers' character and competence issues- or to design adequate risk control policies*".[24]

This lack towards risk assessment definitely compromised the company's ability to prevent and detect fraud. In fact, fraud risks increases when management teams are not able to detect, evaluate and prioritize risks whether they are operative or non-operative risks. Also, acquisitions based on the quantity and not on the quality, such as group synergies or secure return on investments definitely increases the possibility of fraud occurrence. Unfortunately,

[23] Extraordinary circumstances: The journey of a corporate Whistle-blower, p 175,
[24] Clarke T., *International Corporate Governance-a comparative* approach, 2nd edition, 2017

what WorldCom lacked at that time were the right people and the right tools to effectively manage its risk exposure and to pursue its strategic goals.

3.3.5 Information and communication

One of the main reasons of WorldCom's accounting scam success was the lack of information and communication within the company. As stated in the COSO framework, Information is needful for the organization to continue exercising internal control responsibilities to support the achievement of the entity's predefined objectives. Communication instead, represents a process which aim is to provide, obtain and share important information. It can be both Internal and External. While internal information relates to the dissemination of information throughout the whole organization, external information provides important pieces of information to external parties as a response to expectations and requirements. This is what the COSO framework suggests in order to support companies in the internal control implementation. However, this was not what happened in practice within WorldCom.

First of all, the different geographical allocation of WorldCom's several departments made it difficult to disseminate information throughout the entire company. As the previous chapter highlighted, the Human Resource department was in Florida, the accounting department in Texas while the Law department in D.C. This type of configuration and the lack of proper integration did not actually encourage the flow of information within the company. Many employees described WorldCom as an isolated "silos" where each team was aware of its own costs and revenues, but it was actually unaware of other teams' ones. Sharing of information totally lacked. Also, everyone within WorldCom, from employees working in the mail room to executive members, reported that they had never met Bernie Ebbers before. Furthermore, CEO Bernie Ebbers has always been reluctant to use any type of technological mean to get in touch with its employees, for instance he never communicated through emails. This type of approach created a sort of communication gap between employees and CEO.

Communication of key financial information failed also to exist. In fact, the latter was shared only among a very narrow circle of senior executives. Even though it is legitimate to have confidential information which should not be disclosed, WorldCom extended this concept into concealing important information to people who needed to know. Considering how the accounting adjustments have been made, it was clear that the top level was not willing to share such information with other members of the company. For instance, in a discussion between the Director of General Accounting Yates and controller David Myers happened in

May 2001, the former stated "*we 'Took' $327M[illion] of the [MCI Balance Sheet] reserves in the 2nd Q[uarter] of last year. They [MCI personnel] DO NOT know this.*"[25] The same happened with consolidated financial information which was shared only among the most senior levels while concealed to officers who should be normally included.

Access to information was totally restricted. For instance, several times Cynthia Cooper asked for documents to support her work, but she has never been given any complete and correct document. About this, in 1999 she requested a copy of the Monthly Revenue (MonRev) report which was supposed to give a picture of WorldCom's revenues for a given period in support to her Internal Audit project. However, the report was available only among top managers. In fact, at the end of each quarter managers met and discussed on how to close the existing gap between the actual company's revenues and the expected ones. For obvious reasons, top managers were reluctant to show such report to the Internal Audit Department. This is why CFO Sullivan wrote an email to the accounting employee Ronald Lomenzo to make sure Cynthia Cooper was not given the total picture of the report.

3.4 The Fraud Triangle: Factors to explain the case

Understanding WorldCom's operating context and its weaknesses under the COSO framework is fundamental to analyse how specific elements have impacted on WorldCom's members actions and decisions. In fact, there are several reasons that led WorldCom's fraud scam to occur. Each of these can be explained by the analysis of the Fraud Triangle theory which has already been analysed in the first chapter of the paper. When introducing his theory Donald R. Cressey stated that "*Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.* [26]

Therefore, as previously seen, Fraud is not a casual event rather three main elements are always simultaneously present: Pressure, Opportunity, and Rationalization. Each of these elements can be concretely applied to WorldCom's fraud case.

[25] Dennis R. Beresford, *Report of Investigation*, March 31,2003

[26] Donald R. Cressey, *Other People's Money* (Montclair: Patterson Smith, 1973) p. 30

Pressure can be defined as the motivation to indulge into illicit actions. Within WorldCom pressure occurred in several different ways both from the external and internal context:

- Pressure exercised by the market.

  As the company was days away from having to release its financial result to the public, pressure was intense. Showing such low earnings was totally unacceptable. In fact, each year executives of public companies issue an earning guidance, an informal report, which is used to officially predict their companies near future profits or losses. This type of report can affect the recommendation of stock analysts and investors. In fact, based on past results, current information, and also other factors, usually analysts make predictions on the expected profits of firms. Of course, share price reflects those analysts' expectations. Therefore, failing to meet expectations would have caused a downgrade of analyst's opinion on the company and consequently a decrease in stock price. For a company that depends on its high stock price to acquire companies this would have meant falling into a downward spiral. Not to mention that CEO Bernie Ebbers managed to make large purchases just through the help of loans that used WorldCom's stocks as a collateral. Therefore, such a pressure from market expectation led executives to start projecting financial statement's manipulations. For instance, in 1988 the Chairman of the US SEC voiced his concerns on this type of pressure stating what follows: "..*While the problem of earnings manipulation is not new, it has swelled in a market that is unforgiving of companies that miss their estimates. I recently read of one major US company, that failed to meet its so-called 'numbers' by one penny, and lost more than six percent of its stock value in one day.*"[27]

- Pressure form Stakeholder.

  Considering the company's apparent growth through the years, there were high expectations among all stakeholders. Banks, investors, clients, suppliers all relied on what the company was doing. To have an idea, WorldCom in that period represented the fifth most widely held stock in the US and was also considered the first for returns to shareholders over a ten-year period. This was the main reason why WorldCom could not disappoint stakeholder's expectations. Losing banks trust would have meant losing financings to continue all business activities. As a consequence,

[27] Payne, Robb 1999, p.372

investors would have sold WorldCom's shares at very low prices, further contributing to WorldCom's failure.

- Top-down Pressure on employees.

  When CFO Scott Sullivan rationalized that the cost of telling the truth about the company's actual earnings was too high, he exercised great pressure among David Myers to meet the earnings guidance. This pressure has been reversed on the two mid-level accountants who were the only ones to have access to the accounting entries in the system. The two felt extremely uncomfortable and under pressure, however, not following orders could have meant losing their jobs. As Cynthia Cooper wrote in her book, jobs in Jackson (Mississippi), were not easily replaceable. In fact, if someone had concerns about what they observed they often did not report the concerns because they feared losing jobs. This happened especially in Mississippi where WorldCom was the largest and highest paying employer. Furthermore, the two were also very confident about Scott's abilities and they both thought he was smart and highly regarded. Considering how trusted and well respected he was within the industry; he must have known what he was doing. Again, there was a great focus on revenues and on keeping the level of costs down. Employees were constantly denigrated in public when CEO Bernie Ebbers did not accept their findings or their considerations regarding costs.

- Pressure exercised by competitors.

  As stated in the previous chapters, in the late 90s the telecom industry experienced one of the most massive booms in the history. The easy access to cheap capital, due to very low interest rates, determined a rush to expand networks. All companies aggressively invested in infrastructures in order to satisfy anticipated growth in customer's demand. Despite this great competition, WorldCom managed to be the fifth most widely held stock in the US. The company most closely competed with AT&T's Business and Consumer units as well as with Sprint. Of course, this competitive environment created a great pressure on profit margins and on the ability to keep the competitive advantage gained through the years. All these external factors came into play and represented a motivation to indulge in financial statement manipulation. For instance, WorldCom presented in its earnings release substantially higher revenue growths with respect to AT&T and Sprint.

The second element of the triangle is probably the most important one, considering that within WorldCom there were plenty of opportunities to indulge into fraud. First of all, there was a totally ineffective “control environment”. As the previous chapters showed, Control Environment represents all the procedures and standards to carry out internal control within the organization. However, as previously stated, CEO Bernie Ebbers was totally projected towards next acquisitions. He did not have time to release codes of conducts and encourage ethical behaviours within the company. The only message coming from the top was the reflection of his aggressive strategy and its propensity to take risks into the market.

Linked to the control environment, there was a great lack of internal controls. This represented a perfect opportunity for CFO Scott Sullivan, the controller David Myers, and CEO Bernie Ebbers. In fact, by acquiring more than 60 fast-growing companies, WorldCom never managed to fully integrate each companies’ systems and procedures. For instance, the company had more than 60 billing systems instead of having just a single one, which generated confusion and also increased the possibilities to indulge into fraud considering the number of employees having access to the system. This lack of integration gave the opportunity to conceal important information within the company such that financial information was shared only among a closed circle of senior executives.

Again, the internal audit department’s role was totally underestimated and also understaffed. This culture rooted from the top and was spread all throughout the company. It gave David Myers the opportunity to intentionally cut the audit teams system access. By doing so, the controller had the chance to keep Cynthia Cooper’s team from finding the fraudulent accounting entries. Had CEO Bernie Ebbers took the action to create a clear culture to encourage ethical behaviour and to give the right importance to the Internal Audit department this perhaps would not have happened. Also, the subjective judgment involved in the financial statement lines which had been manipulated gave perpetrators the opportunity to conceal the scheme for very long time.

The third and last element of the fraud triangle theory is Rationalization. As explained in the second chapter Rationalization represents an ex-ante process used by perpetrators to try and lower their inner sense of guilt. As highlighted in the report to the Nations, most times perpetrators are first time offenders who lack any criminal background. In fact, the analysis in the report to the Nations on the number of frauds occurred states that 86% of fraudsters has never been punished or convicted to fraud before the crimes reported in the study. WorldCom’s scam is the perfect representation of such findings. In fact, neither CEO Bernie

Ebbers nor CFO Scott Sullivan nor Controller David Myers have ever indulged in such illicit actions before.

But what were perpetrator's justifications to commit fraud? Both mid-level accountants who manipulated the accounts were told that it would have been just a one-time thing. They rationalized their actions by thinking that it was their last time, considering also that CFO Scott Sullivan promised to revise the next quarter's earning guidance so that no one had to make bad entries in the future. They were just taking orders from the top and merely trying to adjust someone's mistake. The idea was that things would have gone better, and numbers would have turned around. No one had the idea of how devastating the consequences for fraud could have been, probably due to the fact that they were committing a non-violent crime. Perpetrator's idea was that they were not harming anyone, even though later on it turned out that, as a consequence, all investors lost their money and all their savings.

3.5 Aftermath of the scandal

Fortunately, WorldCom represented the last big USA fraud at the time. This is not to say that there would be no other frauds, but not of that size. The short succession of USA accounting scandals, such as Enron and only few months later WorldCom, generated from the public a strong need to restore trust in the market. WorldCom definitely gave the final push to reform. In fact, both scams led to dramatic bankruptcies and deeply harmed shareholders who invested billions of dollars in the two companies. Stakeholders, companies' personnel, and investors who suffered tremendous losses were asking for more strict laws, regulations and also listing standards. If corporate executives could not be trusted to ensure transparency and to protect shareholder's and employee's interests, then the Government would have to step in.

In such a scenario, precisely in 2001, the COSO initiated a project in order to evaluate and improve company's enterprise risk management. Therefore, in 2001 the body issued the Enterprise risk management framework already introduced in the second chapter of the paper. It is important to recall that the new framework did not replace the IC-IF rather it incorporated the internal control framework within it. Among these new introductions, in 2002, the United States Congress passed The Public Accounting Reform and Investor Protection Act 2002, better known as Sarbanes-Oxley Act (SOX), which represented a step forward in the evolution of the financial reporting. The Act was signed into law in July 2002 by President Bush who stated: "*Every corporate official who has chosen to commit a crime can* *expect to face the consequences*". The new law was comprehensive and also revolutionary such that it comprised eleven sections that mainly delt with the public company accounting oversight board, improvement in financial disclosure, corporate responsibility, analyst conflicts of interests and auditors' independence. The law required public companies to maintain systems of control and it required auditors (independent auditors) to test the effectiveness of the systems and management teams to certify them. Clearly, this represented a dramatical change in the financial reporting landscape. In fact, both WorldCom and Enron lacked in important areas of reporting, risk assessment and fraud detection.

The Act provided greater support to internal auditors, and it also helped external auditors to better focus on their audit methodologies in order to prevent fraud. Furthermore, the BOD resulted more independent and actually more focused on understanding all types of potential risks that a company might had faced and not just the financial ones. In particular, section 404 of the law focused on auditing practices. It provided that management teams and BOD reported on the reliability of the entity's internal control systems. The aim was to give more importance on the speed and the reliability of the internal control systems while concentrating less on numerical data. By doing so executives and board members would have had a better appreciation of the importance of implementing a strong internal control structure. About this, in an interview to the Fraud magazine concerning WorldCom scam, Cynthia Cooper stated that some of the new SOX measures could have prevented the fraud: "*It is, of course, theoretical, but I think some of the entity-level controls such as having an effective ethics office and independent fraud hot-line could have had an impact."*[28]

Among the most important changes brought by the SOX was the introduction of the Public Company Accounting Oversight Board (PCAOB) a governmental entity created to set auditing, quality control and ethics standards. The Act required the Board to have five members totally independent from any kind of relationship with public accounting companies. Each of them must have had a good knowledge of internal controls, accounting principles, financial statements and also audit committees' responsibilities. In addition, just two out of five must have been Certified Public Accountants (CPAs). Therefore, the Board was provided with the authority of inspecting the work of registered accounting entities and with taking disciplinary actions in case companies failed to comply with the law. By doing so the PCAOB ensured quality reporting to all companies' investors. Therefore, the creation of

[28] Elisabeth Bumiller*, Bush signs Bill Aimed at Fraud in Corporations*, New York Times, July 31, 2002. A2.

the body acted as a deterrent to reduce the number of fraudulent acts. Furthermore, in order to avoid power abuse, the body was positioned under the SEC's review and oversight.

Here is where the interrelation between the COSO frameworks and the 2002 Act becomes important. In fact, SOX act, COSO ERM and COSO IC frameworks all have dependencies on each other. Considering its broad acceptance, the Internal-control integrated framework continues to stand the test of time and it is actually used to satisfy the reporting requirements of the Sarbanes-Oxley Act. Besides, the occurred fraud scams are the result of a profoundly changed context such that the current scenario is dominated by increasingly interconnected components. New risk factors, unknown in the past, have emerged. These of course, have contributed to raise the uncertainty of the economic system, making the traditional method of business management increasingly inadequate. Therefore, with the introduction of the ERM framework, which includes the concepts and components initially developed in the IC-IF, the COSO offered companies a suitable control tool to address the problem of complexity. However, while the SOX emphasises on the control over the financial reporting, the ERM framework adds more elements of risk management which go beyond internal controls, such as the management analysis of risk appetite and risk tolerance in order to achieve the company's objectives.

By now it should be clear that a strong awareness of fraud and fraud prevention is critical to an organization success. Certainly, WorldCom's fraud case served as a lesson to implement several changes within organizations. Companies should have zero tolerance for fraud and mean it. About this, executives are finally being held accountable and no difference should be made in disciplinary actions between employees and executives. Furthermore, organisations should consider publicizing the prosecution of employee fraudsters in order to show a strong culture of compliance and the zero tolerance towards fraud.

Conclusion

The analysis of WorldCom under the COSO framework, coupled with the aftermath of the scandal allows us to reflect on the measures and the models introduced in the fight against fraud. Typically, as discussed in the third chapter, once a fraud scam has occurred there is an extensive media interest, followed by specific investigations, and the urgent need to restore accounting regulations with more calls for actions by governments. This is exactly what happened after WorldCom's scam. The USA government's legislative response was the introduction of the Sarbanes-Oxley Act (SOX) coupled with the upgrade of the ERM and IC-IF COSO frameworks. However, as evidence shows, even after the WorldCom scam, the phenomenon of fraud still prevails. For instance, in Italy in 2003 the failure of the two companies Giacomelli and Parmalat gathered a significant amount of attention and resulted in a scandal. While the former was held responsible for falsifying revenues and overstating inventories, the latter was accused of falsifying earnings, assets, and debts. Similarly, just one year later, in 2004, the software house Finmatica went bankrupt due to the falsification of revenues and overstatement of intangibles. Moreover, today, according to PWC's 2020 global economic crime and fraud survey, 47% of companies reported experiencing an instance of fraud in the past 24 months, with this result being the second highest reported level of fraud incidents in the past 20 years. Considering that the survey's sample includes 5000 respondents from 99 countries, the 47% statistic is cause for great concern. Unfortunately for businesses, fraud is an ongoing issue, and crime rates remain at an all-time high. The close sequence of scandals that has occurred just after WorldCom (regardless of the introduction of legislative measures), in addition to PWC's recent findings should make us reflect on the way in which threats are being assessed. Are the measures introduced up to now really effective to contrast fraud? The numbers reported within PWC's 2020 global economic crime and fraud survey as well as the scams that took place immediately after WorldCom are the proof that the introduction of frameworks such as COSO IC-IF and ERM are certainly necessary models to mitigate the problem, although they have proven to be insufficient to definitively defeat it.

This reasoning though, can be extended also towards other related topics. A parallelism could involve tax evasion. For instance, in September of each year the Committee established by the Decree of the Minister of Economics and finance, chaired by Prof. Enrico Giovannin, issues the “Non-observed Economy” report. This specific report measures the gap between taxes and contributions actually paid, and taxes and contributions that taxpayers should have paid in a regime of perfect compliance with tax and social security obligations under the current legislation. Looking at the evolution of the fiscal gap over the years and taking into consideration the amended measures introduced to avoid evasion, one would expect a decrease in the fiscal evasion. However, it is almost impossible not to notice how the trend of numbers reported today are still very high. For instance, in 2016 the total amount of unpaid Vat corresponded to €35 million, while in 2017 the unpaid amount reached €36 million. Clearly, all the measures introduced to prevent and fight tax evasions over the years have proven to be insufficient to cut tax fraud to zero. Again, we can conclude by stating that normative systems are of course necessary, but not sufficient tools.

Probably, at this point, it is necessary to question the lack of effectiveness of the models and frameworks implemented up to now. History is likely to repeat itself. In fact, each time a legislation is enacted, perpetrators are always able to circumvent the new rules through advanced methods. Therefore, while governments still focus on frameworks to reduce the potential for fraud and creative accounting, priority should be given to another problem that underlies fraud crimes, namely the problem of a low level of ethics in the way business is conducted. More and more legislation can be enacted, but when top executives are motivated by greed and fail to commit to ethical principles, law becomes totally ineffective. In fact, all scandals related to bribery, asset misappropriation, and narratives like Bernard Madoff’s Ponzi scheme, Enron, and WorldCom, are known to have been the product of misconduct in business, also referred to as “low business ethics” by the general public. At a first glance, business and ethics seem to be unrelated. About this, Ethics can be defined as the set of moral principles which affect how people take decisions. When applied to the business context it denotes the study of how a company should act in face of ethical dilemmas and controversial situations. From the examination of this paper, it is clear that fraud and accounting scandals are perennial problems resulting from basic human nature, and that corporate collapses have been the key drivers of most of the accounting scandals occurred. Failure of humans to comply with ethical principles has produced negative effects not only at an economic level, undermining the global economy itself, but also at a legal level, highlighting deep deficiencies in the legislation of almost all governments in the world. Moreover, under a psychological level, non-compliance has undermined the confidence of savers and investors. This is why we can conclude that ethic and business are intrinsically entwined. Therefore, fraud prevention efforts should be addressed also towards the modification of the way in which executives conduct business. Considering that fraud will never be completely eradicated and that companies must adhere to limited budgets, managers should take strategic decisions regarding fraud prevention efforts. For instance, education is at the basis of an honest corporate culture such that statistics have shown that educating employees helps to reduce the occurrence of fraud and increases the likelihood of detecting it. Also, to ensure the implementation of a sound ethical culture, managers should exhibit integrity and transparency in everything they do, such that creating a culture should be a long-term project and not the result of a few months of compliance. There is no ethical policy stronger than the leadership provided by top executives of a company.

In light of what was previously said, we can conclude that fraud management is not a simple process. Unfortunately, there is no single method, technique, framework, or law that is able to prevent fraud. All measures introduced have proven to be insufficient to deal with this phenomenon. This is why a high degree of importance should be given to the combination of discipline, education, and modelling of ethical behaviour in order to prevent and reduce fraud.

Bibliography

[1]. A. Javiriyah, *The accounting fraud at WorldCom the causes, the characteristics, the consequences, and the lessons learned*, (2011).

[2]. A. F. Dalkiliç, *Fraudulent Financial Reporting Techniques: Analysis of Accounting and Auditing Enforcement Releases*, International Journal of Contemporary Economics and Administrative Science, Vol. 7, pp. 224-242, (2017).

[3]. B. Lyke, M. Jickling, *WorldCom: The accounting scandal,* CRS Report for Congress, (2002)

[4]. C. Cooper, *The journey of a corporate whistle-blower – Extraordinary circumstances*, Wiley (2008).

[5]. D. Caplan*, Internal controls and the detection of management fraud*, Journal of Accounting research, Vol. 37, No.1, Spring 1999.

[6]. D. Dragomir, M. Vesna, S. Vladimir, *The role of a company's internal control system in fraud prevention, University of Information Technology and Management*, Vol.11, pp. 34-44, (2015).

[7]. D. T. Wolfe, D. R. Hermanson, *The Fraud Diamond: Considering the four elements of fraud*, CPA Journal 74.12, pp. 38-42, (2004).

[8]. E. Mc Clam, *WorldCom's former finance chief says he cooked books with Ebbers*, The Seattle Times, (2005).

[9]. E. Ocansey, J. Ganu, *The Role of Corporate Culture in managing Occupational Fraud*, Research Journal of Finance and Accounting, Vol. 8, No. 24, (2017).

[10]. Educational Material, Audit course at HEC Management School of Liege, Prof. Yves Francis, 2019-2020.

[11]. E. Bumiller*, Bush signs Bill Aimed at Fraud in Corporations*, New York Times, July 31, (2002).

[12]. F. Schiller, G. Prpich, *Learning to organise risk management in organisations: what future for enterprise risk management?*, Journal of Risk Research, 17:8, pp.999-1017, (2013).

[13]. G. Duffield, P. Grabosky, *The psychology of fraud*, Australian Institute of Criminology, No. 199, March 2001.

[14]. G. Pogliani, N. Pecchiari, M. Mariani, *Frodi aziendali: forensic accounting, fraud auditing e litigation*, Egea (2012).

[15]. G. Svensson, G. Wood, *A model of Business Ethics*, Journal of Business Ethics, pp. 303-322, (2007).

[16]. H. U. Westhausen, *The WorldCom Fraud under a COSO magnifier*, Fraud Magazine, April-March 2010.

[17]. J. T. Wells*, Corporate Fraud Handbook: Prevention and Detection*, Wiley (2011).

[18]. J. T. Wells, *Why employees commit fraud*, Journal of Accountancy, February 2001.

[19]. J. C. Coates, *The Goals and Promise of the Sarbanes-Oxley Act,* Journal of Economic Perspectives, Vol. 21, No.1, pp. 91-116, (2007).

[20]. J. Homer, D. Katz, *WorldCom Whistle-blower Cynthia Cooper*, CFO Magazine, Human capital & Carriers, February 2008.

[21]. J. K. Sidak, *The failure of good intentions: The WorldCom fraud and the collapse of American telecommunications after deregulation*, Yale Journal of regulation, Vol 20:207, (2003).

[22]. K. Johnstone, C. LI, K. H. Rupley, *Changes in corporate governance associated with the revelation of internal control material weaknesses and their subsequent remediation,* Contemporary Accounting Research, Vol. 28 No. 1, (Spring 2011), pp. 331-383.

[23]. K. Oliveira, M. Mèxas, M. Meirino, G. Drumond, *Critical success factors associated with the implementation of enterprise risk management*, Journal of Risk Research, 22:8, pp. 1004-1019, (2019).

[24]. L. W. Jeter, *Disconnected: Deceit and Betrayal at WorldCom*, (2003).

[25]. L. W. Vona, *Fraud risk assessment*, Wiley (2008).

[26]. M. J. Jones, *Creative Accounting, Fraud and International Accounting Scandals*, Wiley (2011).

[27]. M. Anaclerio, A. Miglietta, R. Salvi, F. Servato, *Internal Auditing – Una professione in continua evoluzione*, II edizione (2011),

[28]. M. R. Young, *Financial Fraud Prevention and Detection: Governance and Effective Practices*, Wiley (2013).

[29]. M. J. Comer, *Investigating Corporate Fraud*, Taylor & Francis group (2019).

[30]. M. Samociuk, N. Iyer*, A short guide to fraud risk: Fraud Resistance and Detection*, Taylor & Francis, (2010).

[31]. M. Erikson, M. Hanlon, E. L. Maydew, *Is there a link between executive equity incentives and accounting fraud?*, Journal of Accounting research Vol. 44 No.1, March 2006.

[32]. M. Tran, *WorldCom accounting scandal*, The Guardian, (2002).

[33]. M. S. Beasley, *An empirical analysis of the relation between the Board of Director composition and Financial Statement fraud,* The Accounting review, Vol. 71, No.4, pp. 443-465, (1996).

[34]. M. K. McShane, A. Nair, E, Rustambekov, *Does Enterprise Risk Management Increase Firm Value?,* Journal of Accounting, Auditing & Finance, pp. 641-658, (2011).

[35]. R. E. Cascarino, *Corporate Fraud and Internal control workbook: A framework for prevention,* (2012).

[36]. R. Provasi, *Le dinamiche evolutive del sistema di controllo interno. Dalle origini al framework Coso ERM 2017,* Giappichelli editore, (2020)

[37]. R. Kassem, *The New Fraud Triangle Model*, Journal of Emerging Trends in Economics and Management Sciences, pp. 191-195, (2012).

[38]. S. Clegg, M. Kornberger, C. Rhodes, *Business Ethics as Practice*, British Journal of Management, Vol. 18, pp. 107-122, (2007).

[39]. S. A. Lundqvist, *An exploratory study of Enterprise Risk Management: Pillars of ERM*, Journal of Accounting, Auditing & Finance, Vol. 29(3), pp. 393-429, (2014).

[40]. S. Albrecht, C. Albrecht, *Fraud examination & prevention*, (2004).

[41]. S. G. Sutton, *Learning from WorldCom: Implications for fraud detection through continuous assurance*, Journal of emerging technologies in accounting, Vol. 3, (2006), pp- 61-80.

Sitography

[1]. ACFE, *Report to the Nations – 2020 global study on occupational fraud and abuse*. Available at: https://www.acfe.com/report-to-the-nations/2020/

[2]. AICPA, *Management Override of Internal Control: The Achille's Heel of fraud prevention*, 2016. Available at: https://www.aicpa.org/forthepublic/auditcommitteeeffectiveness/downloadabledocuments/achilles_heel.pdf

[3]. ANAC, *La corruzione in Italia (2016-2019): numeri, luoghi e contropartite del malaffare*. Available at: https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Anticorruzione/MisurazioneTerritorialeRischio/RELAZIONE%20+%20TABELLE-rev3.pdf

[4]. IFAC, www.ifac.org

[5]. COSO, www.coso.org

[6]. CONSOB, *Lo scoppio della bolla delle c.d. Dot-com*, https://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom

[7]. KPMG, *Global profiles of the fraudster, White collar crime present-future,* 2013. Available at:https://assets.kpmg/content/dam/kpmg/tr/pdf/2017/01/global-profiles-of-the-fraudster-v2.pdf

[8]. PWC, Internal Control Environment, Key considerations & Developments, 2014, https://www.pwc.com/gr/en/events/assets/internal-controls.pdf

SEC, *Report of the investigation*, www.sec.org

[9]. PCAOB, *AS 2401: Consideration of fraud in a Financial Statement Audit*, https://pcaobus.org/oversight/standards/auditing-standards/details/AS2401

[10]. Deloitte, www2.deloitte.com

[11]. Forbes, *The rise and fall of Bernie Ebbers*, https://www.forbes.com/2002/04/30/0430wcom.html?sh=7f164ccc1b9a

[12]. MEF, *Documento di Economia e Finanza 2020*, http://www.dt.mef.gov.it/it/news/2020/nadef_2020.html

[13]. IBE, www.ibe.org