52a

Title: STILL FRAUD… AFTER FOLLOWING COSO PROCEDURES

- a *literature review* -

Alcina de Sena Portugal Dias,
Coordinator Professor of Audit, Director of Master Degree in Audit
ISCAP- P.P.

Track: Audit

Keywords: financial scandals, COSO, IIA, fraud concept, fraud models

Title: Still Fraud… after following COSO procedures
- a *literature review -*

ABSTRACT

The objective of this article is to look at the conditions of fraud and its relation to uncovered - risks and/or internal control procedures.
The financial scandals were a real motivation for COSO and its guidelines comprehend the main risks that organizations presently face. Besides, the document On Risk 2021 from IIA – Institute of Internal Auditors must be referred. Usually, uncovered risks are windows open to fraud which will be explained under a theoretical scope of analysis – triangle, diamond and pentagon models. At last a final conclusion based on COSO, IIA risks and fraud occurrence in the organizations will be done.

Introduction

This paper intends to look at COSO principles as something crucial for the achievement of any audit (particularly as concerns Enterprise Risk Management - ERM) and its contribution to risks and fraud minimization. For this, in the item number 1. the financial scandals will be named as contributing to the development and implementation of more procedures in the internal control of the organizations. In item 2. COSO will be considered as a guideline for the enterprise supervision as to internal control and from it, ERM – Enterprise Risk Management, version dated 2017, will be displayed. Next issue, point 3. will just consider fraud and the associated academic models of explanation and issue number 4 will consider fraud and expected risks. At last, in item 5, a conclusion will be made.

1. Big Financial scandals (USA, 2001/2003)

Enron, Parmalat, Worldcom among many others were financial frauds that shocking the finance world deceived the stakeholders promising high dividends for something that was worth nothing at all (Merton, Peron,1993; Anomaly *et al* 2014; Donaldson, Preston 1995). Companies using fraudulent devices tried to increase profits on behalf of the dissimulation of the debt, the false increase of the assets value, schemes that constructed accrued income thus facilitating good profits and high dividend distribution. High dividends make the shareholders happy and greedy for more and more. Companies do feel happy too because people want to get inside them and

buy their capital. Thus, money comes in and shareholders are glad because they get more and more money. Yet they do not pay attention to the accuracy of the disclosure of the financial statements. They just believe in it and all the people involved in their process. Until someone shows some evidence about reality revealing that the financial statements disclosed by the company are not true at all. This way, stakeholders are defrauded (Donaldson, Preston 1995). Their expectation is one and the reality seems to be quite different. These events were violating the main ideas of the following theories:

Table 1 Financial scandals and the violation of the principles

Theories	Literature source
ACCOUNTING	*Ahmed, 2004; Wolk et al, 2008*
CORPORATE SOCIAL RESPONSIBILITY (CSR)	*Dion, 2001; Frynas, Stephan, 2015*
POLITICAL ECONOMY	*Anomaly et al, 2014*
LEGITIMACY	*Suchman, 1995*
STAKEHOLDER	*Donaldson, Preston, 1995*
INSTITUTIONAL	*Bruton et al, 2010*
ETHICS	*Dion, 2001; Frynas, Stephan, 2015*
BUSINESS	*Merton, Peron 1993*

As to the Accounting theory all the principles associated to the preparation and elaboration of the financial statements were broken and overpassed (Ahmed, 2004; Wolk *et al, 2008).* This way if the disclosure of the financial statements is not trustful the CSR theory (Dion, 2001; Frynas, Stephan, 2015) is also being outraged. The stakeholders (Donaldson, Preston, 1995) have been deceived and this has in impact on companies that crosses all directions - the society, the shareholders, the employees, the government and other. As companies fail and go to bankruptcy all the principles and ideas that literature refers about economic and political principles (Anomaly *et a*l, 2014) are put aside. All the concepts and ideas to be considered in order to rule effectively an organization are violated and this has hard consequences on the business (Merton, Peron, 1993) as a whole. By the end one could question as well the principles of legitimacy (Suchman, 1995) when considering that the right things on the right place were not working at all. This means that the values, tradition and culture of the organization were put aside and the inherent hierarchy was violated. So this leads us to the institutional perspective (Bruton *et al*, 2010) and the ethical issues (Dion, 2001) remain the most relevant effects.

These events contributed to a shake on the financial American market. And this can be considered under a *PESTES* analysis perspective that includes the political, economic, social, technological, environmental and sustainable perspective. Under these circumstances and scope of analysis, SEC - Securities Exchange Commission of USA and all the representative associations of accounting, auditing and management among others felt the emergency of reinforcing the measures of internal control in the organizations.

2. COSO - Committee of Sponsoring Organizations of the Treadway Commission

The financial scandals, essentially those occurring from 2001 in the USA, made some hard reaction on the supervising financial entities. COSO – Committee of Sponsoring Organizations of the Treadway Commission, impelled by SEC - Securities Exchange Commission, issued procedures and guidelines for the reinforcement of the organization´s internal control and risk management. Let us look at COSO evolution since its creation (table 2).

Table 2. *COSO - Committee of Sponsoring Organizations of the Treadway Commission*

	1934	**1985**	**1992**	**2001/02**	**SOx 02**	**2003**	**2006**	**2013**	**2017**
USA	SEC	COSO (start)	COSO Control Framework	**Big financial scandals**	Sarbannes Paul, Oxley Michael (*USA Senators)* = SOX ACT IFRS and ISA's	IFAC Credibility Report IFRS and ISA's	COSO Financial Reporting IFRS and ISA's	Integrated framework revision of 1992 internal control	ERM process substitutes CUBE
EU and World				**Bigt financial scandals**	Canadian Bill 198, Loi sur la Secutité Française, Turnbull Guidance UK,	European Directives about Internal control	European Directives	European Directives	European Directives

					J-SOX (2007) Japan IFRS and ISA's	IFRS and ISA's	IFRS and ISA's	IFRS and ISA's	IFRS and ISA's

First it is important to clarify the name of this Committee, devoted to make companies responsible for the preparation, elaboration, reporting and disclosure of their financial statements. COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission). The first chairman of the National Commission was *James* C. Treadway, Jr., Executive Vice President and General Counsel. Paine Webber Incorporated and was a *former Commissioner* of the U.S. Securities and Exchange Commission. Treadway Commission was originally jointly sponsored and founded by five main professional accounting associations and institutes headquartered in the United States:

American Institute of Certified Public Accountants	**AICPA**
American Accounting Association	**AAA**
Financial Executives International	**FEI**
Institute of Internal Auditors	**IIA**
Institute of Management Accountants	**IMA**

The Treadway Commission recommended that the organizations sponsoring it should work together to develop integrated guidance on internal control. These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission - COSO developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. It included representatives from industry, public accounting, investment firms, and the New York Stock Exchange. In 2002 the *control framework* was issued by COSO at the same time that Sox act was in force. Again by COSO in 2006 the *Financial Reporting* was considered and by 2013 the COSO control framework dating back to 1992 was updated.

In 2016 COSO reviewed the final paper entitled *Aligning Risk with Strategy and Performance* about ERM and the output came out in 2017.[1] The following objectives as to strategy and the role of ERM were redefined:

Table 3. New objectives of COSO ERM 2017

Objetives
Enhance alignment between performance and ERM
Accommodate expectation for governance and oversight
Recognize globalization and need to apply a common albeit tailored approach
Present new ways to view risk in setting and achieving objectives in the context of greater complexity
Expand reporting to address greater transparency
Accommodate evolving technology

In brief one can say that this update retitles the framework as Enterprise Risk Management—Aligning Risk with Strategy and Performance, it recognizes the importance of strategy and entity performance and delineates between internal control and enterprise risk management integrating enterprise risk management with decision making. One may think that now COSO ERM may be answering to some questions, suggestions and criticisms from literature. The new figure for COSO will not be anymore the famous Cube but this new one (Figure 1):

[1] In parallel to all these measures of reinforcement of the internal control the worldwide dissemination and implementation of IFRS (International Financial Reporting Standards) and ISA (International Standards on Audit) became something crucial for the global harmonization of accounting and reporting.

Figure 1. ERM 2017

Source: https://commsrisk.com/new-coso-erm-framework-out-for-comment

The transformation of the COSO ERM cube in a COSO ERM process makes a new approach of risk management: a process that is a way of transforming the inputs into outputs. (Williamson,2007). It means that the perspective of ERM for any kind of organization has an input of deep knowledge of the mission, vision and core values of the organization what becomes crucial for grasping the risks associated at the tone of the top. This belief usually is got from the top management combined with the good management of the resources of the organization – human and material - will enhance a good performance. To reach this increased performance we must take care and look at the organization under a risk framework perspective: risk governance and culture associated to the top of the hierarchy; risk strategy linked to objective setting connected to the strategic business units; risk in execution meaning that risk found in the areas or sectors is being treated; risk information communication and reporting should inform all the parties involved in the organization about the state of art of the specific and related risk environment; at last this process of risk analysis makes a final evaluation of its existence – it shall monitor the enterprise risk management performance. Perhaps this will be a hard part to be reached. To perform effectively ERM a large and deep risk analysis must be done because the points and reasons for events presenting a risk are so many and so different that when an evaluation of a risk is done another may emerge that was not previously estimated. Yet this new COSO ERM seems to be quite different from the previous one.

By 2021 COSO is much concerned about digital management risk. It is said by this entity that the audit reports should consider topics such as cyberattacks, blockchain and compliance risks. According to the World News we might say that presently it seems to be true.

Yet, at this point of analysis one could ask: after having described so many procedures to rule the internal control of any company why do frauds appear? How can they surpass so many barriers and obstacles?

3. **Frauds**

SAS 99[1] describes three conditions typically present when fraud is committed: incentives/pressures, opportunities, and attitudes/rationalizations (these are reminiscent of the three sides of the renowned Fraud Triangle). Specifically, the perpetrator of the fraud likely is under pressure or has an incentive to commit the fraudulent act. Second, opportunities probably exist for the perpetrator to commit the fraud. Finally, the perpetrator is likely able to rationalize his or her fraudulent act or possesses an attitude that the act was acceptable. There is a direct relationship between the existence of the three conditions and the likelihood of the occurrence of fraud.

The great difference between a fraud and an error is the predisposition for acting under a suspicious way. We fail or we do mistakes or we do errors because we are human and we can miss some event without having this previous idea. Yet, when we predict, when we estimate and design a failure with a goal that usually becomes a value benefit for us it means that we are trying to do a fraud. Frauds will appear when risks are not duly mitigated and prevented. Fraud will include diverse elements: words, laws, best practice guides, risk maps, websites, compliance officers, text books, regulatory judgments and many more — have a trajectory of formation. This trajectory begins with auditing and expands into risk management, regulation and security more generally. Fraud risk management emerges as a highly articulated, transnational web of ideas and procedures which frame the future within present organizational actions, and which intensify the responsibility of senior managers (Power, 2013). Frauds will emerge when the internal control of the companies is weak, for instance when the invoicing department is leaded by someone that is responsible at the same time for the cash/treasure department as well. This may suggest a conflict of interests with guaranteed dividends. These are events can occur in any company, for

[1] SAS 99, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants —AICPA— in October 2002. The original exposure draft was distributed in February 2002. SAS 99, which supersedes SAS 82, was issued partly in response to contemporary accounting scandals at Enron, WorldCom, Adelphia, and Tyco. SAS 99 became effective for audits of financial statements for periods beginning on or after December 15, 2002.

instance along the leaf time when the personnel are on vacation leave and someone has to fulfill two functions or more at the same time that can be matched together and grant some good benefits to the perpetrator. The opportunities are present we just need a plan to profit them (to rationalize) and a good reason to do it (pressure/motivation).

Hall (2011) defines fraud as anything that denotes a false representation of a material fact with the formal intention of deceiving and inducing the other party to deeply rely on the fact. According to general *Common Law*, a fraudulent act must meet the following five conditions:

(i) False representation — there must be a false statement or a nondisclosure;

(ii) Material fact — a fact must be a substantial factor in inducing someone to act;

(iii) Intent — there must be the intent to deceive or the knowledge that one statement is false;

(iv) Justifiable reliance — the misrepresentation must have been a substantial factor on which the injured party relied; and

(v) Injury loss — the deception must have caused injury or loss to the victim of the fraud.

In the business environment, fraud is an intentional deception, misappropriation of a company's assets, or manipulation of its financial data in order to get advantage of the perpetrator (Hall, 2011). Usually when speaking of accounting literature, fraud is also commonly known as white-collar crime, defalcation and irregularities dealing with the financial statements of the organizations. As to some relevant economic sectors, besides the financial ones and the big organizations, and particularly in the food retail distribution, Spink et al. (2017) stressed that there is a relevant need to implement an effective risk management plan in order to prevent fraud. In this sense, Spink et al. (2019) mentioned some steps for an efficient and effective food fraud policy-making implementation:

(i) establish the definition and scope;

(ii) define food fraud as a food agency issue;

(iii) publish an official government statement focused on prevention (e.g., law, regulation, rule, guidance);

(iv) support and fund the policy implementation; and

(v) continue to evaluate and adjust the response. For fraud prevention/detection in any kind of organization the auditors along the development of their work can follow these guidelines.

Furthermore, and speaking about the auditor's work in a company, fraud may be found at two different levels: on behalf of the employee or on the management (Hall, 2011). We can find employee fraud as to the organizations when the internal control procedures inside in their

operation process are not quite well implemented and workers know better than anyone how to take advantage of it.

Suh, Nicolaides and Trafford (2019) considered the effects of reducing opportunity and fraud risk factors as to the occupational fraud in financial institutions. They referred that usually fraud occurs on behalf of the people that work day by day on tasks fulfilling functions, which enables them a deep knowledge of the connected whole process. This is the ideal for committing a fraud — to know the holes and limits of the process. When we speak about the top management one must say that fraud is usually related to the absence of ethics.

Boyle, DeZoort and Hermanson (2015) considered the impact of the fraud model used and its relation with the auditor's judgements. As we will see along this article different fraud models can be considered and their context is related to the structure and the environment of the organization. In order to understand and explain fraud and among the different perspectives that one may construct three of the most cited models from literature are going to be considered — triangle, diamond, pentagon.

3.1 Theoretical Models for Fraud analysis

a) Triangle Model

Fraud triangle theory is the first one capable of explaining the elements that cause fraud. This theory is presented by Cressey in 1953 but one must stress that it still keeps applicable. The fraud triangle elements consist of pressure, opportunity, and rationalization.

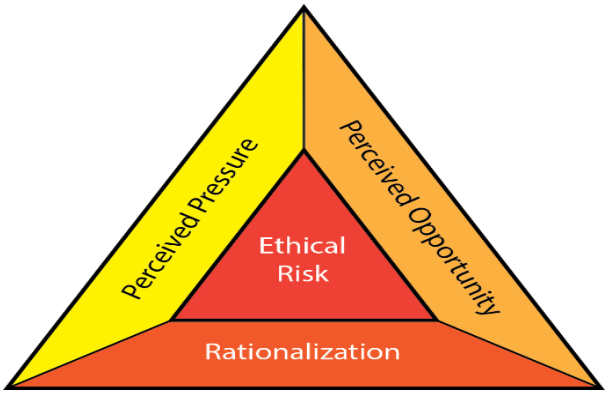

Figure 1. Fraud Triangle Model

Source: httpshttps://commons.wikimedia.org/wiki/File:Fraud_Triangle.png

All these elements combined try to explain fraud occurrence. The pressure may mean the need that someone has, or feels that has, or is obliged to do something on a particular situation of life

that many times hides any common sense. This situation is revealed as an opportunity to do an event that arises when the author thinks realizes some good advantages of it and thus, it will be worth doing and this is the rationalization or the design of the fraud to be committed.

b) Diamond Model

Yet in some situations the combination of these factors may explain the fraud but other times some capability to do it is important as well. If one looks at the Big Financial Scandals dating back to the early 21st century like Enron, Parmalat and WorldCom, it is clear that people who created them, besides the pressure, the opportunity and the rationalization they had the capability to do it (Abdullahi and Mansor, 2015). They understood the business process quite well and knew easily what they could do in deception. As to this interpretation we could associate the diamond model presenting this new characteristic — the capability.

Figure 2. The diamond model

Source:
https://www.google.com/search?q=FRAUD+DIAMOND&rlz=1C1GCEA_enPT846PT847&oq=FRAUD+DIAMOND&aqs=chrome..69i57j0i22i30l9.3072j0j7&sourceid=chrome&ie=UTF-8

Yet, we must be very careful when making generalizations because frauds depend on many variables. For instance if we look at literature, authors like Zaini, Carolina and Setiawan (2015) found different results but as to the academic environment: they showed that pressure, on a student's perspective, has positive and significant effect on academic fraud behavior enabling the triangle model.

Fraud diamond elements (opportunity, rationalization, pressure or incentive and capability) do not explain it. According to Wolfe and Hermanson (2004), it is impossible for deception or fraud to occur if no one has the right capability to perpetrate the deception or fraud. The said capability is an individual quality to commit deception, which drives them to find an opportunity and make use of it. Yet one must argue that it depends on the type of activity we are considering. The fraud triangle model may be adequate for the analysis of student's fraud but the administrative staff of a University need already some capability or competence to do a fraud — arising the diamond model. With more variables in the course we find the Pentagon Model.

c) Pentagon Model

Fraud pentagon concept was named by Crowe (2011) who added the arrogance dimension to the diamond analysis. For him a person will commit acts of cheating due to pressure, opportunity, rationalization, competence and arrogance. Arrogance is an attitude of superiority as to the rights or pertained position from an individual who feels that he/she is beyond any control or institutional policy of the company. Arrogance is an exaggeration shown by someone or a reflection of pride due to his/her position. If someone has a high arrogance and a good company's position, then he will be more likely to commit fraud.

Figure 3. *Fraud pentagon theory*

Source: https://www.researchgate.net/figure/Fraud-pentagon-theory_fig1_341646159.

This model replaced the capability — identified in the Diamond Model, for competence and added the arrogance factor. It seems that to do a fraud some competence and arrogance associated are needed. Competence because it is necessary to understand quite well and to know the process

of the business where the fraud is going to occur in order to determine the weakest points of its controls. The arrogance usually can be found in the high level of hierarchy — top management— that pretend to be unquestionable and this way they feel at ease to perpetrate the fraud. Crowe (2011) suggested the pentagon model reflecting five attributes (opportunity, pressure, rationalization, arrogance and competence) that may frame a fraud event. Taking again the above mentioned example of the Big American frauds, for instance we might still argue that perhaps these elements were present — the arrogance of the top management and the competence of the auditors both very much associated with a big lack of ethics. One could ascertain it with the Diamond Model as to the capability of the fraud players yet it may be more clearly explained through the joint of arrogance and competence which lead to the Pentagon Model.

So, as far as literature goes we cannot say for sure that there is one model that fits it all. There are too many variables that together can explain a fraud according to its type and nature and to a particular theoretical approach.

The goal addressed at the beginning of this paper was to match the controls to be followed by companies adopting COSO as to some of the risks that the organizations do not see or consider and these may become frauds.

Some authors argue that some use of data mining techniques could help to prevent financial fraud (Ngai *et al*., 2011;Kirkosa *et a*l.). One could take into account the big data fraud risk management process that some group companies like Alibaba have pursued as to fraud (Chen et al., 2015). It is quite interesting to see what the companies use in order to face fraud what usually takes into account the management risk analysis of the company.

3.2 Expected Risks and Fraud

According to IIA – The Institute of Internal Auditors, in America, issued in the year end of 2020 their perspective of Risks for 2021 that are not so much different from present risks (in 2022).

This document is *IIA OnRisk 2021.* From its analysis, along this study, it was condensed and enabled the elaboration of a single table. In his table the main risk was named Cybersecurity having influence in the internal and external risk of the organizations. So under the umbrella of Cybersecurity the related risks - Information, Third Party, Management, Sustainability, Disruptive – were considered and the other risks were either external or internal.

Table 4. Cybersecurity – the umbrella for all the risks

Main risk	Other risks
Cybersecurity Information, Third Party, Management, Sustainability, Disruptive	**External** Economic and Political **Internal** Governance, Talent, Culture, Going Concern

Source: author own elaboration from On Risk 2021.

Cybersecurity

Computers have done incredible things for our lives and will increasingly continue to do so, however we must also learn to protect ourselves. We need not guard against the technology itself, but rather those who wish to pervert it for personal gain or others' pain. Under the threat of global terrorism and organized crime we must come to understand that cyberspace is truly a digital battlefield and has real-world consequences when critical infrastructure is directly affected. We must not forget to stay vigilant and we must always keep running (Dustan, 2016). One of the major challenges associated with cyberspace is the lack of national boundaries, enforceable rules/treaties, and internationally recognized regulatory committees (Chayes, 2015).

Criminals and adversaries are able to cross space and time anonymously and with complete disregard for geopolitical boundaries, making active cyber defense problematic. International law dictates that retaliation in self-defense is an acceptable use of force, however it becomes tricky when attacking an enemy's system which technically violates another nation's sovereignty (Flowers and Zeadally, 2014).

To add another layer of complexity, attackers routinely relay network traffic around the world through thousands of nodes, making it virtually impossible to identify the originating system with absolute certainty and requiring defenders to cross countless borders to find the perpetrator. Subsequently, to deter an attacker a government entity may need to relay malicious network activity across uninvolved nations' telecommunications networks and noncombatant systems, creating a legal quagmire (Hathaway et al., 2012).

The security on the information produced and got/sent/in stock through Internet is something crucial at present. If the organizations/institutions are considered it means that we are just referring all the types of stakeholders information given and received— internal and external. The risks associated have already been before mentioned and frauds may occur due to — opportunity, pressure, rationalization, arrogance, easy access and competence and many other variables like

the ethics (or its absence). At this point we could create a fraud model heptagon that follows the pentagon created by Crowe (2011) and just adds the attribute “easy access” or “absence of ethics” because computers are a kind of asset that is quite easy to get and presently is something basic for committing a fraud and if ethics is not embedded in the agent, if it does not make part of the behavior of the person — the field for fraud is open and free. Citing Gengler (1999), and as to frauds related to recent cyber issues we can name some from the end of 20th century: the US-based Computer Security Institute, in its fourth annual survey and the FBI, reported that corporations, banks and government agencies all face a growing threat from computer crime committed both inside and outside the organizations. For the third straight year, financial losses due to computer security breaches mounted to more than $ 100 million. And for the third year in a row, system penetration by outsiders increased and 30 % of respondents reported intrusion. Those reporting their Internet connection as a frequent point of attack rose from 37 % in 1996 to 57 % in 1999. This was around the end of last century!

Presently we agree with Vogel (2016) when it is said: the current consensus is that there is a worldwide gap in skills needed for a competent cybersecurity workforce. This skills gap has implications in the national security sector, both public and private. Although the view is that this will take a concerted effort to recover it, it presents an opportunity for IT professionals, university students, and aspirants to take jobs in national security — national intelligence as well as military and law enforcement intelligence. As to the emerging employment trends, some of the employment challenges and what these might mean in practice, these are good issues to be considered. In order to close the cyber skill gap by taking advantage of this window of opportunity, one must allow individuals interested in moving into the cybersecurity field to do so, via education and training (Fay, Negangard,2017).

Virtual worlds are computer-generated, immersive environments where participants interact with others while engaging in social, entertainment, and economic endeavors. To illustrate how virtual worlds can be used to study fraud, Dilla et al. (2013) examined the documented virtual world fraud cases using the “fraud diamond” model (Wolfe and Hermanson, 2004) and their findings have real-world implications regarding the causes and prevention of fraud. They include:

(i) perpetrator motivations often lead to nonmonetary achievement and manipulation, as well as financial gain;

(ii) fraud victims tend to have misplaced trust and overestimate the capability of fraud prevention governance mechanisms;

(iii) participant-designed record-keeping systems may protect corporate assets from theft; and

(iv) virtual worlds may serve as a laboratory for evaluating risk management strategies.

This research illustrates how parallels between fraudulent behaviors in virtual and real worlds can advance our understanding of fraud antecedents (Dilla et al., 2013).

Cyber fraud must be executed by people with very special technical informatics skills. Thus, in order to explain them it seems adequate to place this issue under the diamond fraud model once the main attributes associated are: the pressure/motivation, the opportunity, the rationalization and mainly the competence or technical skills — capability— needed to do it. This is a situation that may happen in the external and internal market, in other words, this is a global phenomenon that can affect any type of business, either public or private, in any country provided the lack of ethics (Demidenko, 2010).

According to the document of IIA (*OnRisk 2021*) we can register risks as to the board information and sustainability. As to reasons that can explain their occurrence one might argue that either the theoretical approach of the diamond or pentagon fraud might explain it. This is so, because both theories state that the pressure/motivation, the opportunity, the rationalization and the capability or the competence can explain fraud event. Yet sometimes the arrogance (in the pentagon theory) is used by people to achieve the frauds with some property as if they could be assigned to do so and no one could question them for doing it. We can give as examples the situation when the top management is involved in the fraud engineering and its safe and "clean" power position is openly assumed and exhibited towards the hierarchy.

Disruptive innovation is a kind of risk we must be prepared to face: it seems that due to market conditions or to some restraints of different nature like the pandemic ones we are suffering presently many organizations must have the capability to change their mission and start again with a new product or service, or else they will go in a bankruptcy.

Other Risks

External

The economic situation of the country is a consequence of the global political and economic status either imported from EU, Asia or USA. Countries that are rich and have money can get resources in a better quality and price, in better conditions, and can face risks in a different way. We might consider all these risks as having an external origin with reflection and implication in the internal environment of the country and particularly in the life of the organizations.

Internal

This way, internally in the organization, issues like the governance, the talent safeguard, the culture and the continuity of the company or the "going concern" idea, will be the issues to be

considered as risks. Any of these risks can be inserted under the theoretical frame of a triangle, a diamond or a pentagon fraud. Their happening and positioning will have to do with the step where they stand within the organization.

4. Conclusion

The aim of this paper was to consider the connection between COSO procedures and fraud. First a brief evolution of COSO was done naming the main perspectives issued by that entity in order to face risk. Then on a risk perspective according to *IIA – On Risk 2021* risk was considered and its relation to fraud comprehension was done on a theoretical basis of analysis.

Trying to give an academic answer to the questions we did across this article, citing: *after* h*aving described so many procedures to rule the internal control of any company why do frauds appear? How can they surpass so many barriers and obstacles?* we are now summarizing some of these ideas in the below described Table 5 assuming that fraud can happen within any type of organization from the low level till the up level management but being more likely to occur in the level **bold underlined** due to the models characteristics.

Table 5. COSO, IIA and Fraud theoretical Models

COSO INTERNAL CONTROL (main parts)	**RISKS: IIA *ON RISK 2021***	**Possibility of fraud**	***Triangle model***	***Diamond model***	***Pentagon model***
ENVIRONMENT	Cybersecurity External and internal	HIGH	UP LEVEL MEDIUM LEVEL **LOW LEVEL**	UP LEVEL **MEDIUM LEVEL** LOW LEVEL	**UP LEVEL** MEDIUM LEVEL LOW LEVEL
RISK ANALYSIS	ERM 2017 and risk minimization	MEDIUM	UP LEVEL MEDIUM LEVEL **LOW LEVEL**	UP LEVEL **MEDIUM LEVEL** LOW LEVEL	**UP LEVEL** MEDIUM LEVEL LOW LEVEL
CONTROL ACTIVITIES	Cyberattack can happen	HIGH	UP LEVEL MEDIUM LEVEL **LOW LEVEL**	UP LEVEL **MEDIUM LEVEL** LOW LEVEL	**UP LEVEL** MEDIUM LEVEL LOW LEVEL
INFORMATION	Cyberattack can happen	HIGH	UP LEVEL MEDIUM LEVEL **LOW LEVEL**	UP LEVEL **MEDIUM LEVEL** LOW LEVEL	**UP LEVEL** MEDIUM LEVEL LOW LEVEL
MONITORING	May be compromised	HIGH	UP LEVEL MEDIUM LEVEL **LOW LEVEL**	UP LEVEL **MEDIUM LEVEL** LOW LEVEL	**UP LEVEL** MEDIUM LEVEL LOW LEVEL

COSO main parts related to the good functioning of any kind of organization comprehend the environment – internal or external meaning: Business knowledge, the organization culture, the scope of approach of all environmental variables that can interfere in the day by day of the organization. The risk analysis should be related to the functioning – operational, tactic and strategic of the organization. A stress on the control of all the activities should guarantee trustfulness as well as a good system of reporting the company´s relevant information. Monitoring is a quite an important activity that ckecks and validates the procedures implemented. If all these steps are followed the organization has a sound internal control.

Yet, even having these procedures implemented the organizations can face risks that are unexpected. These risks were named by IIA as a pandemic (COVID) consequence. Mainly the Cibersecurity that can affect all the steps (COSO) described. There is only an expected medium Risk if ERM – Enterprise Risk Management is followed otherwise all the other issues of the internal control, may register a High probability of occurrence of fraud. And this may happen in any kind of organization an at any level of the hierarchy. Yet, considering the assumptions of the three models considered – triangle, diamond and pentagon – one can say that they may be associated to the level of management: triangle suggests the low level of management – the need, the occasion and the rationalization; diamond relates probably more to the medium management on behalf of the item capability; at last pentagon is associated to the top level of the management because of the factor arrogance. Nevertheless these are only some ideas collected from the international scandals profile. One may be able to find a triangle model in a fraud done by the top management and a pentagon model associated to a fraud committed by the workers of a factory!

As an answer to the question embedded in this study one might say that unfortunately frauds will continue to be frauds. Fraud keeps on arising in spite of all the internal procedures and guidelines existing in an organization There are many other variables that can explain it, as ethical principles, character traits and many other individual specific situations, and these reasons stay out of the procedures written about the internal control of any organization.

However the more controlled we get an organization through the implementation of internal control procedures the harder it is to deceive its process and more time and ability or capacity is needed to think about how to do it.

Limitations of the study

This article is just a literature review as to internal control and COSO, risks and fraud and has no opinion of the companies about this so did not yet reach this phase. We might say this is a work in progress.

Paths for future investigation

Based on the described theoretical models used to explain fraud one could do interviews in the organizations to locate fraud under the triangle, diamond or pentagon models and trying to locate it in the hierarchy of the organization. Then after collecting the results one should see if the model of fraud selected and the level of management associated can explain the fraud in order to validate (or not) the conclusion of this paper.

References

Abdullahi, R. and Mansor, N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent for Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *5*(4), 38-45.

Ahmed, R. (2004) Accounting Theory, 4th Edition, U.K, Business Press Thomson Learning

Anomaly, J., Brennan, G. (2014). Social Norms, The Invisible Hand, and the Law. University of Queensland Law Journal 33 (2).

Boyle, M., DeZoort, T. and Hermanson, D. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, *34*(6), 578-596.

Bruton, G., Ahlstrom, B. and Li, H. (2010) Institutional Theory and Entrepreneurship: Where Are We Now and Where Do We Need to Move in the Future? Entrepreneurship Theory and Practice, 3 (3) 421–440

Chayes, A. (2015). Rethinking Warfare: The Ambiguity of Cyber Attacks. *Harvard National Security Journal*, *6*(2), 474-519.

Chen, J. et al. (2015). Big data based fraud risk management at Alibaba. *The Journal of Finance and Data Science*, *1*(1), 1-10.

Cressey, D.R. (1953). *Other people's money: a study in the social psychology of embezzlement*. Belmont, USA: Wadsworth Publishing Company.

Crowe, H. (2011). *Why the Fraud Triangle is No Longer Enough*. Retrieved from www.crowehorwath.com.

Demidenko, E., McNutt, P. (2010). The ethics of enterprise risk management as a key component of corporate governance, International Journal of Social Economics, 37 (10), pp.802-815, doi: 10.1108/03068291011070462

Dilla, W., Harrison, J. and Mennnecke, E. (2013). The assets are virtual but the behavior is real: an analysis of fraud in virtual worlds and its implications for the real world. *Journal of Information Systems*, *27*(2), 131-158

Dion, M. (2001), 'Corporate Citizenship and Ethics of Care: Corporate Values, Codes of Ethics and Global Governance', in J. Andriof and M. McIntosh (ed.), Perspectives on Corporate Citizenship (Greenleaf, Sheffield, UK), 118–138

Donaldson, T., Preston, L. (1995) The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications Academy of Management Review, vol. 20 (1), 65-91

Dustan, J. (2016). *U.S. Critical Infrastructure Cybersecurity: An Analysis of Threats, Methods, and Policy-Past, Present, and Future* (Graduate Thesis). University of South Carolina, Columbia, USA.

Fay, R. and Negangard, E. (2017). Manual journal entry testing: Data analytics and the risk of fraud. *Journal of Accounting Education*, *38*, 47-49.

Flowers, A. and Zeadally, S. (2014). US Policy on Active Cyber Defense. *Journal of Homeland Security and Emergency Management*, *11*(2), 289-308.

Frynas G., Stephan S., (2015) Political Corporate Social Responsibility: Reviewing Theories and Setting New Agendas, International Journal of Review Management, 17(4), pp. 483–509

Gengler, B. (1999). Cyber attacks from outside and inside. *Computer Fraud & Security*, *5*, 6-7.

Hall, J. (2011). *Accounting Information Systems*. Boston, USA: Cengage Learning.

Hathaway, O.A. et al. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 817-885.

Kirkosa, E., Spathis, C. and Manolopoulos, Y. (2007). Data Mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995-1003

Merton, R., Peron, A. (1993) Theory of risk capital in financial firms, Applied Corporate Finance, 6 (3), 16–32

.Ngai, E.W.T. et al. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559-569.

Power, M. (2013). The apparatus of fraud risk. *Accounting Organizations and Society*, *38*(6-7), 525-543.

Suchman, MC (1995) Managing Legitimacy: Strategic and Institutional Approaches, Academy Management Review , 20(3) 571-610

Spink, J. et al. (2017). Food fraud prevention shifts the food risk focus to vulnerability. *Trends in Food Science & Technology*, *62*, 215-220.

Spink, J. et al. (2019). The application of public policy theory to the emerging food fraud risk: Next steps. *Trends in Food Science & Technology*, *85*, 116-128.

Suh, J., Nicolaides, R. and Trafford, R. (2019). The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime and Justice*, *56*, 79-88.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32-46.

Williamson, D. (2007). The COSO ERM framework: a critique from systems theory of management control, International Journal of Risk Assessment and Management, 7(8), pp 1089-1119 **doi**: http://dx.doi.org/10.1504/IJRAM.2007.015296

Wolfe, D. and Hermanson, D. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal*, *74*(12), 38-42.

Wolk, I, Dodd, J. and Rozycki J (2008). Accounting Theory: Conceptual Issues in a Political and Economic Environment, 7th edition, Sage Publications Inc. California

Zaini, M., Carolina, A., & Setiawan, A. R. (2015). Analisis Pengaruh Fraud Diamond dan Gone Theory Terhadap Academic Fraud (Studi Kasus Mahasiswa Akuntansi Se-Madura). In Simposium Nasional Akuntansi XVIII, Medan, Indonesia.

On line sites:

COSO ERM 2017 https://commsrisk.com/new-coso-erm-framework-out-for-comment

IIA - ON RISK 2021 “On Risk 2021: A Guide to Understanding, Aligning and Optimizing Risk,” *https://iiabelgium.org/risk/onrisk-2021-a-guide-to-understanding-aligning-and-optimizing-risk/*