ISSN 2389-8186
E-ISSN 2389-8194
Vol. 8, No. 2
Julio-diciembre de 2021
doi: https://doi.org/10.16967/23898186.712

ARTÍCULOS ORIGINALES

Risks and fraud: A theoretical approach

ALCINA AUGUSTA DE SENA PORTUGAL DIAS*

pp. 7-21

* PhD Entrepreneurial Sciences. Instituto Superior de Contabilidade e Administração, Porto, Portugal. E-mail: alcina@iscap.ipp.pt. ORCID: 0000-0003-0860-1102. Google Scholar: https://scholar.google.com/citations?user=XHCHKa4AAAAJ&hl=en.

ISSN 2389-8186
E-ISSN 2389-8194

Vol. 8, No. 2
Julio-diciembre de 2021
doi: https://doi.org/10.16967/23898186.712

COMO CITAR ESTE ARTÍCULO
How to cite this article:

de Sena, A. (2021). Risks and fraud: A theoretical approach. *Revista Perspectiva Empresarial, 8*(2), 7-21.

Recibido: 29 de abril de 2021
Aceptado: 20 de agosto de 2021

ABSTRACT **Objective.** To explain fraud occurrence —under three theoretical models— and apply it to the organization's hierarchy. **Methodology.** Based on the IIA risk outlook for 2021, an exploratory theoretical scope of analysis was constructed. Risks were considered under the umbrella of three fraud theories: Triangle of Cressey; Diamond of Wolfe and Hermanson; and Pentagon of Crowe. **Results.** Fraud occurrence may be explained by the perpetrator's position across the hierarchical organization chart: where it is stressed that arrogance from the Pentagon fits the top management position; competence from the Diamond fits the middle management; and need, opportunity and pressure from the Triangle fit mainly the lower management. **Conclusions.** Fraud was considered under three main models, concluding that it may be explained through different worker motivations related to their management position in the company.

KEY WORDS Risks, fraud triangle, fraud diamond, fraud pentagon, management level.

Riesgos y fraude: una aproximación teórica

RESUMEN **Objetivo.** Explicar la ocurrencia del fraude —bajo tres modelos teóricos— y aplicarlo a la jerarquía de la organización. **Metodología.** A partir de la perspectiva de riesgos de la IIA para 2021 se construyó un ámbito de análisis teórico exploratorio. Los riesgos se consideraron bajo el paraguas de tres teorías del fraude: triángulo de Cressey; diamante de Wolfe y Hermanson y pentágono de Crowe. **Resultados.** La ocurrencia del fraude puede explicarse a través de la posición del perpetrador a lo largo del organigrama jerárquico: destacando que la arrogancia del pentágono se ajusta a la posición de la alta dirección; la competencia del diamante se ajusta a los mandos intermedios y la necesidad, la oportunidad y la presión del triángulo se ajustan principalmente a los mandos bajos. **Conclusiones.** El fraude fue considerado bajo tres modelos principales, concluyendo que puede ser explicado a través de diferentes motivaciones de los trabajadores relacionadas con su posición de gestión en la empresa.

PALABRAS CLAVE riesgos, triángulo del fraude, diamante del fraude, pentágono del fraude, nivel directivo.

Riscos e fraude: uma abordagem teórica

RESUMO **Objetivo.** Explicar a ocorrência de fraude —sob três modelos teóricos— e aplicá-la à hierarquia da organização. **Metodologia.** Com base na perspectiva de risco do AII de 2021, foi construído um âmbito teórico exploratório de análise. Os riscos foram considerados sob o guarda-chuva de três teorias de fraude: o triângulo de Cressey; o diamante de Wolfe e Hermanson; e o pentágono de Crowe. **Resultados.** A ocorrência de fraude pode ser explicada através da posição do perpetrador ao longo do organograma hierárquico: destacando que a arrogância do pentágono se enquadra na posição de gestão de topo; a competência do diamante se enquadra na gestão intermédia e a necessidade, oportunidade e pressão do triângulo se enquadra principalmente na gestão inferior. **Conclusões.** A fraude foi considerada sob três modelos principais, concluindo que ela pode ser explicada através de diferentes motivações dos funcionários relacionadas à sua posição de gestão na empresa.

PALAVRAS CHAVE riscos, triângulo da fraude, diamante da fraude, pentágono da fraude, nível de gestão.

Introduction

Considering the pandemic time, we are living in (which started in March 2019) and on a risk management perspective associated to the theoretical scope of analysis of fraud, this study is going to be based on the forecasts disseminated by the Institute of Internal Auditors —IIA— through the document *OnRisk 2021*, recently issued. This document names the main risks the organizations will be facing in the near future. As it is well known, when risks are not duly and properly considered frauds may emerge. It is an aim of this paper, under a perspective of a theoretical review, to describe and place these risks under the umbrella of the respective studies: triangle of fraud (Cressey, 1953), the diamond fraud (Wolfe and Hermanson, 2004) or the pentagon fraud (Crowe, 2011).

To do so, this study will be organized as follows: first the concept of risk will be associated to the document published by IIA, *OnRisk 2021*. Secondly the description of the abovementioned risk theories will be considered and at last a match between the possible frauds and the respective theoretical approach will be done. To summarize it a brief conclusion will be displayed.

Some expected Risks for 2021

The IIA, in 2020, published *OnRisk 2021: A Guide to Understanding, Aligning, and Optimizing Risk*, which for the first time brought together essential perspectives of boards, management, and chief audit executives (CAEs) —the three key players in risk management—. Through a series of interviews with members of all three groups, along with a survey of CAEs, *OnRisk 2021* offered a unique and insightful examination of the interactions and views of those who most directly affect risk management.

OnRisk 2021 adds key players' views on organizational risk relevance as a factor in measuring alignment. Observations of this year improved the alignment on key risk knowledge and capability and some potential misalignment on how relevant some risks are viewed. The influence of COVID-19 was the most important factor for them. A response to the pandemic contributed to an improved alignment among risk management players on business continuity, risk management, and communications. The pandemic also exposed the strengths and weaknesses of how organizations manage disruption. It was needed to change to adapt to reinvent the soul of the organizations. Yet COVID-19's most influential long-term impact may be the marked by the acceleration of technology's positive and negative effects on cybersecurity, talent management, economic and political volatility and disruptive innovation.

The IIA list of major risks to be faced by organizations in the near future (Table 1) does not cover all the significant risks in every organization; risks excluded from this analysis may have particular relevance —even significant relevance— to organizations, depending on their specific circumstances.

Table 1. Description of IIA risks

Risks	This Risk Considers
1. Cybersecurity	Whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm
2. Third Party	Organizations' abilities to select and monitor third-party relationships
3. Board Information	Whether boards feel confident that they are receiving complete, timely, transparent, accurate, and relevant information
4. Sustainability	Organizations' abilities to establish strategies to address long-term sustainability issues

Risks	This Risk Considers
5. Disruptive Innovation	Whether organizations are prepared to adapt to and/or capitalize on disruption
6. Economic and Political Volatility	The challenges and uncertainties organizations face in a dynamic and potentially volatile economic and political environment
7. Organizational Governance	Whether organizations' governance assists or hinders achievement of objectives
8. Data Governance	Organizations' overall strategic management of data: its collection, use, storage, security, and disposition
9. Talent Management	Challenges organizations face in identifying, acquiring, upskilling, and retaining the right talent to achieve their objectives
10. Culture	Whether organizations understand, monitor, and manage the tone, incentives, and actions that drive the desired behavior
11. Business Continuity and Crisis Management	Organizations' abilities to prepare, react, respond, and recover

Source: author own elaboration.

Consequent to the pandemic time we are living, since March 2020, all the possible work has been done from home. This leads us to think a little about the security of the Internet use as to the information received, produced and disseminated. So in a comprehensive analysis we might associate risks number (1, 2, 3, 4, 5) as to cybersecurity. With this arrangement of issues one aims to get security about the access used in communication, naming cybersecurity (Risk 1) as a main issue.

Presently the organizations current life is conducted through Internet applications like Teams, Zoom, Mobile Apps among others. To control third party services one must contact them using these ways either for consulting, for transportation, for accounting, or just for cleaning services (Risk 2). The information —financial and no financial— that is constructed within the companies depends deeply on the data, got on line, from the different players, so that the financial reports can be done and may enable an accurate information about the company (Risk 3). It is important to utilize the data analysis skills that are proper: the power of Big Data while performing a procedure that is required on all financial statement audits, viz., an analysis of journal entries for potential red flags of fraud (Fay and Negangard, 2017). Besides some other techniques (data mining) can be used in detecting firms that issue fraudulent financial statements —FFS— and deal with the identification of factors associated to FFS (Kirkos, Spathis and Manolopoulos, 2007). And this is related with the sustainability of the organization because it deals with sound financial reports, which present good profits that are applied not only in the former investors but also in the worker motivation and in the contribution to the objectives of the around society thus satisficing all the stakeholders (Risk 4). These times reflect some hard issues as concerns the day after of this pandemic but even in between, companies must reinvent themselves and do a kind of reengineering to face the future and this is being disruptive — breaking some mores in order to reach some solutions and being able to innovate (Risk 5). All these risks to be minimized must be safeguarded by cybersecurity.

Table 2. Main risks associated to Cybersecurity

Main Risk	Consequent Risks
1. Cybersecurity Organizations should be prepared to manage cyber threats that can cause disruption and reputational harm	2. Third Party 3. Boards Information 4. Sustainability 5. Disruptive Innovation

Source: author own elaboration.

Looking at Table 1 we can see that risk 6 is related to the market so we could name it as an external risk. The economic and political volatility are dimensions that cannot be managed by the organizations. Yet they must be duly considered in their current operational work and it is looking at them that the companies must reconsider the Mission, Vision and Strategies and adapt them to the new and unexpected realities.

Table 3. External Risks

Kind of Risk	Consequent Risks
External risks	6. Economic and political volatility

Source: author own elaboration.

All these dynamic and changing variables affect the organization world and they must be sure about the data they receive and the information thereof processed (Risk 8). And in the organizations management process in order to get things right we need the right people in the right place and the most talented ones represent a risk for the companies once they can leave them easily. So a different management of the talents is needed (Risk 9). And this is related to the culture of the organization which translates the mission, values and beliefs of the company (Risk 10), and it is in crisis time that these assumptions can be tested. If the organizations do not pay attention to all the above mentioned risks independently of their origin they will have serious problems as to the business continuity and some bankruptcies may happen (Risk 11).

Table 4. Internal Risks

Kind of Risk	Consequent Risks
Internal risks	7. Organizational governance 9. Talent management 10. Culture 11. Business continuity and crisis management

Source: author own elaboration.

So, in brief, and from the analysis of Table 1 one could get all the risks there explained in a simple table like (Table 5).

Table 5. Cybersecurity as an umbrella risk

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.

At last we can say that Cybersecurity is a great risk to the organizations all around the world. One could say that this is a global issue. And this issue is related and embedded in the internal or external risks as to the organizations. These risks are external because they are related to the global economy and to the policy of each country and are internal when they concern the life of the organizations in terms of culture and governance, talents in their management and continuity of the business activity. Let us consider now the existence of these risks and the possibility of becoming frauds.

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 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

[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.

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 environment of the organization.

In order to understand and explain fraud, in this paper, the three most cited models from literature are going to be considered — triangle, diamond, pentagon.

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.

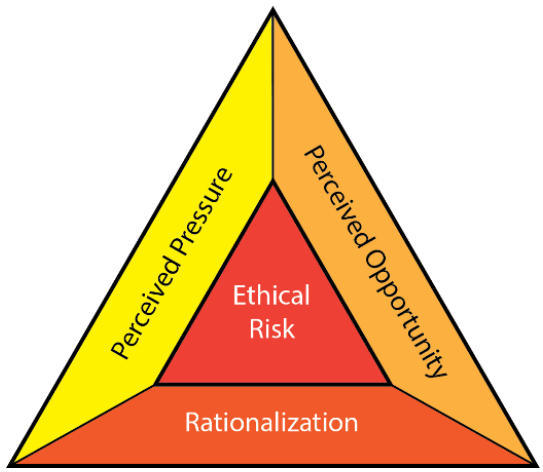

Figure 1. Fraud Triangle Model. Source: https://commons.wikimedia.org/wiki/File:Fraud_Triangle.png.

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.

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://chapters.theiia.org/miami/ChapterDocuments/Raise%20the%20Red%20Flag-%20Lynn%20Fountain.pdf.

Yet, we must be very careful when making generalizations because the 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.

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 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 people— that pretend to be unquestionable and this way 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. They were fitted in the Diamond Model as to the capability of

simulation but moreover they may be explained by the arrogance and competence associated which imply 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 these fraud theories to some of the risks that the organizations may face in the near future. Perhaps according to some authors some use of data mining techniques could help to prevent financial fraud (Ngai et al., 2011). 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 with the aim of avoiding or minimizing it. The next issue will consider fraud and associate it to the before named risks.

Expected Risks and Fraud

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 named, we are just referring all the types of information given and received to all the stakeholders — 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.

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.

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

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. 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.

Triangle frauds will happen most probably at the basic level of this pyramid (figure 4) because they depend on the opportunity, the rationalization and the pressure/motivation. We mention the lowest level because there is not a need for specific expertise but a strong and definite motivation with a fringe benefit connected in order to achieve something valuable — it is like getting basic Internet connectivity the first level of the fraud.

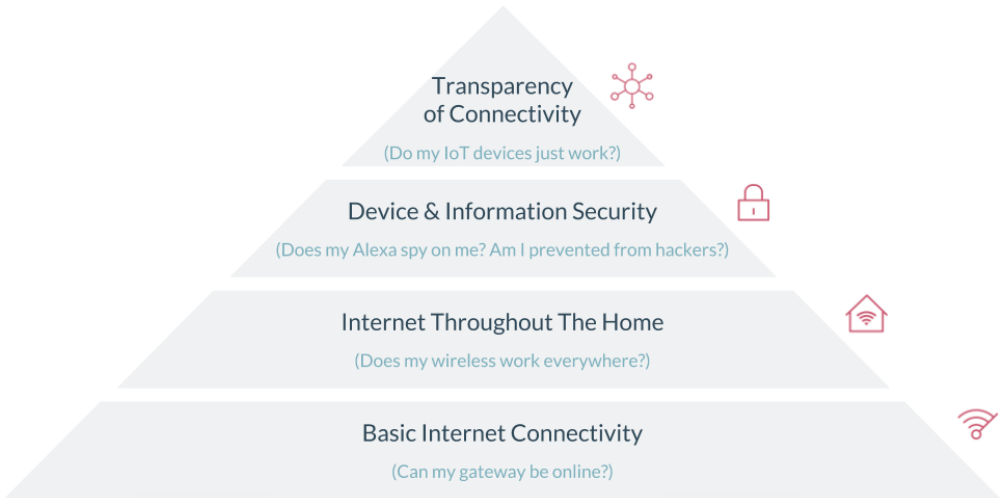

Figure 4. Maslow's Hierarchy for internet and the era of IoT. Source: https://www.minim.com/blog/maslows-hierarchy-for-internet-and-the-era-of-iot.

But when we can get this Internet around the world when we know how to use it —Internet throughout the home— it seems that we have some capability to do it so the diamond fraud can be applied — we have the motivation, the opportunity, the rationalization of the event and the capability.

If we climb up one or two levels more in the flowchart we are getting to the executive area described as Device & Information Security, top management area that should inspire transparency of connectivity.

At both points of the hierarchy we may explain the occurrence of fraud under a pentagon model. This model accrues the attribute arrogance as a kind of defense of the perpetrator because he/she is a kind of people who have power and are arrogant enough in order to disguise the fraud they know they have done or are to be doing. At this time the capability element of the diamond model is replaced by the competence one.

At last and coming back to *OnRisk 2021*, risks as to governance, as to talent safeguard or as to culture all of them may be associated to the profile of the fraud perpetrators: these can be explained through the pentagon, the diamond or the triangle fraud models.

Besides and when frauds happen in the organizations they can compromise their "going concern" principle.

Conclusion

In this study after considering the different risks, named by IIA forecasts for 2021, their possibility of becoming or enabling frauds were considered.

The situations related to these risks may be translated in benefits to the perpetrator. In order to explain the existence of fraud we tried to identify the place where it can happen across any organization

and from its top to the lowest level one can register that at least the fraud models (pentagon, diamond and triangle) may be applied.

So, fraud has been considered, along this study under three different theoretical models: pentagon, diamond and triangle.

All of them have some traits in common — initiative/pressure, rationalization and opportunity. So this way, one can refer that the triangle model is embedded in all the other models because they are primary factors that can explain fraud existence.

Figure 5. Fraud theoretical models related to the management flowchart. Source: author own elaboration.

As referred all the models include the triangle model (placed at the Low level). From this basis if we consider in addition the factor capability the diamond model is built (at the Middle level). From this, under the addition of the arrogance element and replacement of capability for competence, we get the pentagon model (at the Top level).

Considering the world of organizations as a place where frauds are more common and if we look top-down at their hierarchy and associate

them the above mentioned models one can say: the pentagon model due to the elements of arrogance and competence may be related to the top management, the diamond model meaning the capability of performing some special tasks can be associated to the middle management and at last the triangle model may be related to the low management.

Yet, this is neither a scientific proved issue nor a universal truth. We can have a fraud explained by the triangle model placed in the board of any company and a pentagon model explanation for an event occurring at the middle or low management level. We may have frauds in any kind of organization design and we are not able to relate them specifically to the level of management. Frauds are deeply connected to the ethical profile (or its absence) as to the perpetrator, to the kind of business and to the imperfections of the processing flow, many times mainly located in the internal control of any organization.

At this point we come to the limitations of this study and mainly to the future paths for investigation. We might say that this is just a theoretical approach defined by the considered three fraud models and it is well known that there are a lot of variables that can lead to fraud besides them. Ethics is a main element that connected to the cultural framework of the company and even of the country and should be considered.

This way as future avenues for investigation we might consider doing both qualitative and quantitative analysis in different types of organizations with the aim of identifying the factors that can lead to fraud in corporate companies, banks, public institutions, small and medium enterprises.

By the end it would be quite interesting to see what happens to these models after a pandemic time which will have a great impact on the society due to social and economic consequences to be reflected in the organizations and on the workers.

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.

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.

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.

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.

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.

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.

IIA. (2020). *OnRisk 2021: A Guide to Understanding, Aligning, and Optimizing Risk*. Bruxelles, Belgium: IIA.

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.

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.

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.

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

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.