VILNIAUS UNIVERSITETO
VERSLO MOKYKLA

INTERNATIONAL PROJECT MANAGEMENT PROGRAM

Ilona Balsiukaitė

MASTER'S THESIS

Sukčiavimo Prevencijos Sistemų Diegimo Projekto Valdymas	***Project Management During Implementation of Anti-Fraud Software***

Ph.D. Andrius Valickas

Name, surname of the supervisor

Vilnius, 2022

SANTRAUKA

VILNIAUS UNIVERSITETO
VERSLO MOKYKLA
TARPTAUTINĖS PROJEKTŲ VADYBOS PROGRAMA
STUDENTAS ILONA BALSIUKAITĖ
SUKČIAVIMO PREVENCIJOS SISTEMŲ DIEGIMO PROJEKTO VALDYMAS

Magistro darbo vadovas – Ph.D. Andrius Valickas

Darbas paruoštas – 2022 Vilnius

Darbo apimtis - 61 puslapis

Lentelių skaičius - 15

Iliustracijų skaičius - 8

Informacijos šaltinių skaičius – 67

Trumpas darbo aprašymas: Kelis paskutinius metus pastebimas sukčiavimų nuostolių augimas. Augant sukčiavimų kiekiams, sukčiavimų prevencija tampa svarbia užduotimi organizacijoms, patiriančioms nuostolių dėl sukčiavimo atakų. Sėkmingas projektų valdymas yra plačiai autorių išnagrinėta tema. Tačiau sukčiavimo prevencijos sistemų diegimo projektų sėkmė priklauso nuo papildomų specifinių veiksnių, kurie nėra tirti. Šis darbas skirtas apžvelgti sukčiavimo prevencijos sistemas ir jų diegimo projektų principus.

Darbo tikslai ir užduotys: Atlikti sukčiavimo prevencijos sistemų diegimo projektų analizę, įvertinti pagrindines tokių projektų charakteristikas ir pateikti rekomendacijas sėkmingam tokių projektų vykdymui.

Darbe naudoti tyrimo metodai: Teorinei daliai buvo atlikta mokslinės literatūros ir aktualių leidinių apžvalga. Empirinei daliai buvo naudotas kokybinis tyrimas, atliktas interviu su 12 ekspertų.

Atliktas tyrimas ir gauti rezultatai: Ekspertai patvirtino dalies veiksnių įtrauktų į teorinį sėkmingą sukčiavimo prevencijos sistemų diegimo modelį. Ekspertai iškėlė papildomus veiksnius, iššūkius ir specifikas į kurias verta atkreipti dėmesį dirbant su sukčiavimų prevencijos sistemų diegimo projektais.

Pagrindinės išvados: Norint įmonėje sėkmingai įdiegti sukčiavimo prevencijos sistemą, svarbu identifikuoti ir atpažinti įmonės vadovų poziciją ir strategiją dėl sukčiavimo prevencijos. Tai turi reikšmingą įtaką projekto sėkmei. Taip pat svarbu teisingai atsirinkti sistemą, kuri bus diegiama, deleguoti kvalifikuotus resursus, laikytis tradicinių projekto valdymo pagrindų, laikytis etinės lyderystės principų.

SUMMARY

VILNIUS UNIVERSITY
BUSINESS SCHOOL
INTERNATIONAL PROJECT MANAGEMENT PROGRAM
STUDENT ILONA BALSIUKAITĖ
PROJECT MANAGEMENT DURING IMPLEMENTATION OF ANTI-FRAUD SOFTWARE

MA thesis supervisor – dr. Andrius Valickas

MA thesis prepared – 2022 Vilnius

MA thesis scope - 61 pages

Number of tables in Master thesis - 15

Number of figures in Master thesis- 8

Number of references – 67

A short description of Master thesis: In recent years, there has been an increase in fraud losses. As the prevalence of fraud increases, fraud prevention is becoming an increasingly critical task for organizations. Many academics have researched successful project management. However, the effectiveness of fraud prevention system projects is dependent on aspects that have yet to be investigated.

Aims and objectives of Master thesis: to perform research on the anti-fraud software implementation projects, appropriately evaluate the characteristics of such projects, and develop principles and recommendations for the successful completion of anti-fraud software implementation projects.

Methods used in Master thesis: For the theoretical part, a review of the scientific literature and relevant publications was conducted. A qualitative investigation including interviews with 12 experts was employed for the empirical part.

Research carried out and results obtained: Almost all of the elements contained in the theoretical model for the successful implementation of fraud prevention systems were validated by the experts. Additional issues, problems, and specificities that need to be considered while working on fraud prevention system installation projects have been recognized by experts.

Main conclusion: To successfully implement a fraud prevention software in an organization, it is critical to identify and understand the company's management's position and strategy towards fraud prevention. This has a huge influence on the project's success. It is also critical to choose the appropriate software for implementation, to assign competent personnel, to adhere to conventional project management practices, and to adhere to ethical leadership principles.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

During the Global Pandemic in the year 2020, there was a significant increase in the number of fraud attacks and fraud losses. The Global Pandemic was not the root reason for the surge in fraudulent activity. It just accelerated the formation of an atmosphere that was favorable to fraudulent activity. For example, transitioning from physical money, paperwork, and identification to digital money, documentation, and identification. The question of when organizations would become completely remote, with no physical contacts, had been raised, and COVID-19 provided a specific date for when this transition would happen.

In today's world, every organization might be targeted by a fraud attack, and numerous sources emphasize that there is no such thing as fraud immunity. Many businesses are altering their strategies and attempting to adjust to the post-pandemic environment, which is often referred to as the "New Normal" in the corporate environment. In recent years, there has been a significant increase in the desire among businesses to deploy technologies to combat fraud occurrences. It is also important to note that the supply of such technologies is continuously growing.

Even while the history of fraud may be traced back to ancient Greece, the fact is that the disciplines of fraud detection and prevention are relatively new. Therefore, experience and understanding related to fraud are not well researched subjects. Moreover, businesses still have a very limited understanding of fraud, as well as how fraud should be detected and prevented. As a result, implementing technology to combat fraud can be challenging for some organizations.

Project management and effective project management are topics that have been extensively addressed among researchers, and there have been many studies conducted on these subjects. The issues of fraud prevention, detection, and anti-fraud software did not get much attention from researchers, although this is not a completely new field of research. Project management and the implementation of anti-fraud technologies, on the other hand, are two topics that have a research gap between them. This master's thesis is dedicated to assisting companies who are involved in the fight against fraud and who are putting technological solutions in place to do so, as well. The problem statement of this master's thesis is to identify the challenges associated with anti-fraud software technology implementation projects, understand about the complexities of such technology implementation, and determine how such implementation projects should be successfully managed.

Furthermore, the primary aim of this master's thesis is to perform research on the anti-fraud software implementation projects, appropriately evaluate the characteristics of such projects, and develop principles and recommendations for the successful completion of anti-fraud software implementation projects.

The following are the objectives of this master’s thesis:

1. The initial objective is to examine scientific literature in order to comprehend and investigate fraud in general. This investigation will look at the fundamentals of fraud occurrence as well as the strategies that are used to prevent fraud from occurring. Another component of this literature review will be an assessment of anti-fraud technologies and a theoretical overview of what has previously been investigated on this matter. Furthermore, the literature evaluation will also include an examination of the specifics of how the anti-fraud software installation project should be handled and what constitutes successful project management in general. The achievement of the literature research should be the construction of a conceptual anti-fraud implementation project success model, as well as the determination of the primary variables that influence the success of the project.
2. The following objective of this master’s thesis is to develop the methodology for empirical research.
3. The other objective is to conduct empirical research. This research will address the findings from the literature review as well as attempt to discover principles that were not previously identified in the literature review. The research part should determine the requirements of projects for the implementation of anti-fraud technical solutions, as well as the practicality of such projects.
4. The last objective is to conduct an assessment of the theoretical research and qualitative research findings related to anti-fraud software implementation projects. Additionally, to formulate the principles and recommendations for anti-fraud software implementation projects.

The research for this master's thesis begins with a comprehensive literature review on the implementation of anti-fraud software. The literature review assisted in highlighting the relevance of the issue and in preparing for the qualitative research part. The research will be conducted employing a qualitative research methodology — expert interviews.

1. THEORETICAL ASPECTS OF ANTI-FRAUD TECHNOLOGY

The Banks’ Association of Lithuania announced in 2021 that, as a consequence of the Global Pandemic, the amount of electronic fraud in Lithuania had grown by a factor of many times over the previous year. A fraud-related loss of 1.2 million euros was sustained by the organization during the first quarter of 2020, according to association records. Unfortunately, fraud resulted in a loss of 2.9 million euros in the first quarter of 2021, which was the greatest loss ever recorded in the history of the organization (The Banks Association of Lithuania, 2021). Lithuania is not the only country that has seen a rise in the number of reported fraud occurrences in recent years. Around the world, anti-fraud professionals are taking steps to prevent fraud assaults from increasing in number and damaging their organizations. Each year, financial crime results in a total worldwide loss of 3.5 trillion United States dollars due to fraud and embezzlement (Piper, Metcalfe, 2020).

Damage caused by fraud, on the other hand, is not restricted to monetary losses exclusively. Other expenditures that are difficult to quantify include intangible costs such as reputational damage and decreased employee morale (Stamler, Marschdorf, Possamai, 2016). When a business becomes the victim of a fraud attack, the consequences may be tremendously devastating to the organization's reputation. Restoring a company's reputation is time-consuming and costly, both in terms of money and in terms of time. It is also possible that fraud will have a substantial influence on the development of relationships with customers, business partners, or regulatory authorities. Furthermore, it might have a direct impact on other parties involved, such as shareholders, investors, banks, or insurance companies (Mackevicius, Giriunas, 2013).

In recent years, there has been a considerable increase in the number of online transactions, purchases, and other types of online activity. Due to the Global Pandemic, businesses all around the world were forced to become instantaneously remote and accessible online, which accelerated the development of their operations. However, while on the one hand, this fast development provided an opportunity for fraudsters to insist on continuing illegal activities, on the other hand, it presented an opportunity for businesses to start paying more attention and to invest in anti-fraud technologies. Effective anti-fraud technology, in particular, might assist an organization in preventing financial losses, increasing security levels, protecting the organization's brand reputation, and providing better customer service towards its customers.

According to the studies conducted by the Association of Certified Fraud Examiners (2021) and PricewaterhouseCoopers (2020), the number of fraud cases among organizations worldwide is growing in the past years. According to forecasts, the percentages are expected to continue to grow through the year

2022. This, without a doubt, draws attention to anti-fraud software and technologies as well as raises knowledge of their existence and effectiveness. First and foremost, in order to better understand what and how anti-fraud software should be implemented, it is necessary to understand the fundamental causes of fraud, fraud management principles, and fraud prevention and detection approaches. Project management is the process through which organizations put innovative ideas into action and see them through to completion. Project management success indicators, as well as obstacles that may arise during the implementation of anti-fraud software, are some of the subjects that will be addressed in this literature research.

1.1. The Concept of Fraud

The concept of "fraud" has been defined in a variety of ways by different authors and sources. According to the Cambridge Dictionary, fraud is "the crime of getting money by deceiving people". This concept, however, is severely limited by the fact that only money can be obtained. The Oxford Dictionary defines fraud as follows: "wrongful or criminal deception intended to result in financial or personal gain". This is a widely accepted definition of fraud that can be found in a variety of sources, including articles, books, research papers, corporate papers, or training materials. Baesens, Van Vlasselaer and Verbeke on the other hand, provided a more detailed description of fraud. They characterize it as "an uncommon, well-considered, imperceptibly concealed, time-evolving, and often carefully organized crime which appears in many types of forms" (Baesens, Van Vlasselaer, Verbeke, 2015, p. 3). Further to that, authors emphasize that fraud is social phenomenon which has a difficult-to-identify characteristic (Baesens, Van Vlasselaer, Verbeke, 2015). The Association of Certified Fraud Examiners in the broadest sense, describe fraud as any crime committed for financial benefit in which deceit is the principal modus operandi (The Association of Certified Fraud Examiners, 2021). All the definitions include the same keyword, which is "crime", and this is most likely the best word to illustrate what fraud certainly is.

In terms of history, the first known written evidence of deception may be traced back to Ancient Greek times. The earliest documented fraud plan was a scheme to obtain insurance coverage for the high expenses of maritime transportation by making false claims to the insurance company (Economou, Kyriazis, 2017). As of now, the most prominent fraudulent schemes have been Pyramid Investing and other well-known Ponzi schemes, which first debuted in the United States of America in the early 1920s and have spread around the world. Because of these techniques, fraud was brought to the attention of a broader audience and became well known in the financial industry. Pyramid investing schemes were built on investments that provide spectacular profits while posing no risks to the investor (Frankel, 2012). However, the reality is that, instead of receiving a fortune, the investors were defrauded and experienced significant financial losses. These scams, despite the fact that they were decoded, extensively reported in the media, and fraudsters were apprehended and prosecuted, continue to exist in various forms in different parts of the world. The fraud schemes evolve in response to changes in time and technology, becoming progressively innovative. Today's fraudsters are well-versed in a wide range of scams, from identity theft to phishing scams or romance scams, from corporate email compromise fraud to social engineering schemes. Fraudsters also engage in tax evasion, asset misappropriation, cyber security threats, and a variety of other types of fraud. Nevertheless, no matter how many schemes are designed and deployed, the motivations and justifications for engaging in fraud remain consistent.

1.2. The Motivation for Fraud to Occur

The motives and reasons for fraud were firstly reflected by the Fraud Triangle Theory, described by Cressey in 1953. Cressey conducted interviews with imprisoned thieves and recognized three strong similarities in the frauds they perpetrated (Cressey, 1953). Several researchers, including Abdullahi, Mansor (2015), Baesens, Vlasselaer, Verbeke (2015), Davis, Harris (2020), Dellaportas (2012), Dorminey, Fleming, Kranacher, Mackevicius, Giriunas (2013), Riley, Richard (2012), and Sorunke (2004), have researched and analyzed the Fraud Triangle Theory. The most important topic that the researchers tried to answer during their investigations was why fraudsters commit fraud. The Fraud Triangle Theory illustrates and clarifies the basic elements of fraud occurrences. It served as a starting point for further investigations into fraud from a sociological and psychological perspective. As a result, researchers thoroughly continue investigating it.

Motives and justifications for fraud are represented by the Fraud Triangle, which is composed of three of the most important elements - motivation, opportunity, and rationalization – that help to explain why fraud occurs (figure 1). Therefore, a person planning to commit fraud will need to have significant pressure or motive to do so — this might be due to a poor financial condition, a personal crisis, or an intense desire to achieve a financial and/or personal advantage. In the event that legal measures fail to resolve a problem, individuals may begin to contemplate engaging in illicit activity (The Association of Certified Fraud Examiners, 2020). Every fraudulent activity is designed to result in monetary gain or some other kind of advantage for the perpetrator, and this is the fundamental reason for committing fraud (Baesens, Van Vlasselaer, Verbeke, 2015).

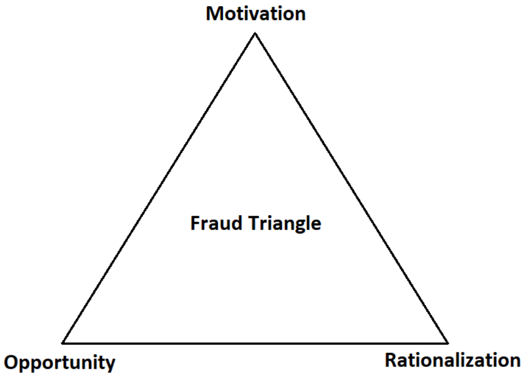

Figure 1. The Fraud Triangle. Composed by the author according to Cressey (1953)

Gender differences may have an influence on aspects that drive motivation. According to Holtfreter's research, men are more inclined to commit fraud in circumstances where they are driven to do so by gambling debt or addiction than they are in situations where they are given other types of incentive. In cases when the same driving force behind women's deception was caused by a financial need to cover medical expenses, or by the illness of a child or spouse (Holtfreter, 2015). Mackevicius and Giriunas also examined the differences between men and women and concluded, that men commit fraud due to motives related to “economic, different types of addictions (alcohol, drugs, gambling, etc.), dissatisfaction with the work and the leaders, and the reputation of being a loser and underestimated” (Mackevicius, Giriunas, 2013, p. 155). Females, in contrast to males, base their choices on personal concerns such as the health of a sibling or child, as well as emotional considerations such as their own feelings and emotions of vulnerability. They may also engage in fraud as a way of revenge, driven by sentiments of anger or jealousy, among other things.

The existence of an opportunity is the second critical component in the occurrence of fraud. A several conditions must be satisfied before fraud could be committed. For example, when it comes to occupational fraud that occurs within an organization, those opportunities could include a lack of provisions, a lack of internal controls, weaknesses in fraud prevention processes, or simply weak points in the organization's software program systems. To put it another way, knowing that the perpetrator will not be prosecuted or that the deception will go undiscovered provides the fraudster an opportunity to commit a crime. Because they are utilized to overcome internal security measures or simply disregard fraud signs, senior management is critical in this situation because they open the door to fraudulent activity (Dellaportas, 2012).

According to the Fraud Triangle framework, the last criterion is rationalization. It may be explained as “justification that unethical behavior is something other than criminal activity” (Hashim, Salleh, Shuhaimi, Ismail, 2020, p. 1149). Baesens, Van Vlasselaer and Verbeke described rationalization as the “psychological mechanism that explains why fraudsters do not refrain from committing fraud and think of their conduct as acceptable” (Baesens, Van Vlasselaer, Verbeke, 2015, p. 8). This demonstrates that the fraudster is searching for a reasonable argument to validate his or her decision to commit fraud and that the consequences are worth it. Personal ethics and societal responsibility, to put it another way, are concepts that are commonly used to describe this concept. It is possible that employee dissatisfaction with their working conditions, benefits, and other aspects of their work experience will serve as a foundation for internal fraud (Davis, Harris 2020).

In addition, the Fraud Triangle Theory, as well as the large majority of other classical theories, have been taken into consideration. Some opponents of the Fraud Triangle Theory acknowledge that the model should take additional variables into consideration (Mackevicius, Giriunas, 2013). Critics or opponents of the Fraud Triangle Theory were Wolfe and Hermanson (2004), who researched the theory and recommended the incorporation of a supplementary factor – capability – as one of the factors to consider. As an additional consideration, they recommended that, in addition to the incentives (or motives) to commit fraud, the opportunity to do so, and the justification (or attitude of the fraudster), the individual's competence to undertake fraudulent activity be taken into account. According to Wolfe and Hermanson, a perpetrator who intends to commit fraud must possess a certain set of abilities and competencies in order to be effective in his or her attempt. This matter was supported by the proven experience in fraud investigations of one of the authors. This unique four-element theory was given the name "The Fraud Diamond Theory" (Wolfe, Hermanson, 2004).

By investigating the relationship between the age of workers who commit internal fraud and the probability of possible loss caused by fraud, Mackevicius and Giriunas have made a significant contribution to the understanding of the importance of competence. Additionally, they emphasized that more experienced employees have a better understanding of the organization's internal controls, are more familiar with additional possibilities, and possess the employee skills and competencies essential to prepare for fraudulent activity (Mackevicius, Giriunas, 2013). According to some researchers, adding a fifth component to the fundamental causes of fraud, such as arrogance, would change the "Fraud Diamond" into the "Fraud Pentagon." When someone demonstrates the characteristic of arrogance, it reveals their inflated ego and feelings of authority, which lead them to believe that they are capable of defying internal restrictions (Ramadhan, D. 2020). The Fraud Pentagon and the Fraud Diamond theories are illustrated in the figure 2 respectively.

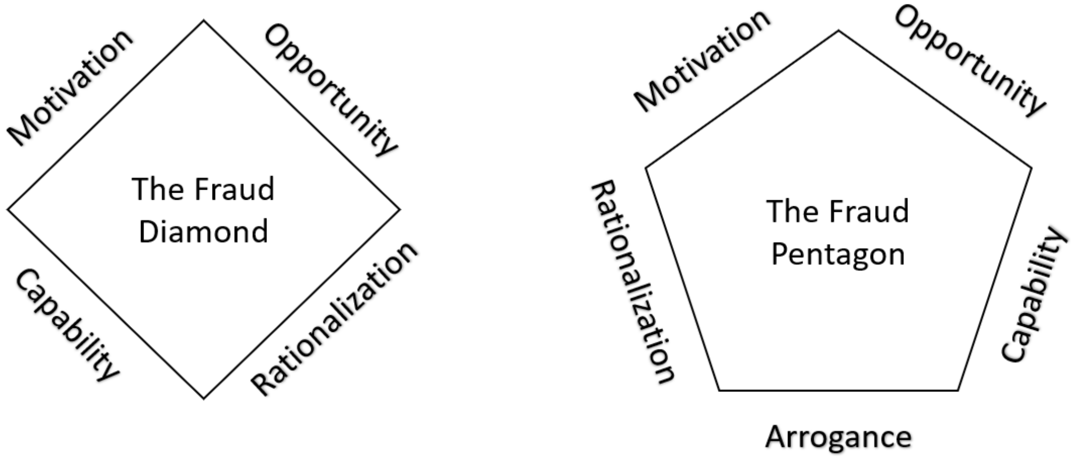

Figure 2. The Fraud Diamond and the Fraud Pentagon. Composed by the author according to Ramadhan (2020) and Wolfe, Hermanson (2004)

Despite the critiques and modifications that have been suggested, the Fraud Triangle Theory continues to be the most fundamental model for explaining the social phenomena of fraud today. In countries across the world, fraud examiners and other professionals continue to depend on Cressey's discoveries, which state that fraud occurs when the components of motivation, opportunity, and rationalization are present.

1.3. Fraud Management Strategy: Detection, Prevention and Response.

In terms of fraud management strategy, there is no one concept that is more accurate than another, such as the Fraud Triangle hypothesis, which is used to determine the fundamental cause of fraud. One way to describe the fraud management strategy is a framework constructed on three main components, like the Fraud Triangle theory, which describes fraud occurrences using three essential features. The three primary components of such a fraud management strategy framework are fraud prevention, detection, and prosecution (Ketz, 2006). Bartsiotas and Achamkulangare proposed a structure that is comparable to the one described above, except that the prosecution component was substituted with a responding component (Bartsiotas, Achamkulangare, 2016).

An even more extensive and comprehensive version of this approach was released by the United States Government Accountability Office in 2015. They offered the Fraud Risk Management Framework, which was built on the foundation of three critical control categories: detection, prevention, and response. Aside from that, the technique is made up of several different components: commitment, assessment, design, implementation, evaluation, and adaptation. Furthermore, the framework emphasizes the need for monitoring and feedback systems throughout the process (U.S. Government Accountability Office, 2015). Amasiatu and Shah analyzed various approaches to fraud management frameworks and suggested their first party fraud management framework, which consists of seven elements – "deterrence, prevention, detection, investigation, sanction and redress, measurement and monitoring, and policy." (Amasiatu, Shah, 2018, p. 356).

As part of his research, Riney investigated and offered an alternative technique for fraud management: a two-step fraud defense system that included components for detection and prevention (figure 3). The fraud triangle technique was employed to highlight potential indicators of threat occurrence for the detection component. The preventative component is based on business excellence models, which are discussed more below. Using business excellence models, you may create a framework for internal controls that is built on defined roles in the areas of leadership ethics, and governance, among others (Riney, 2018).

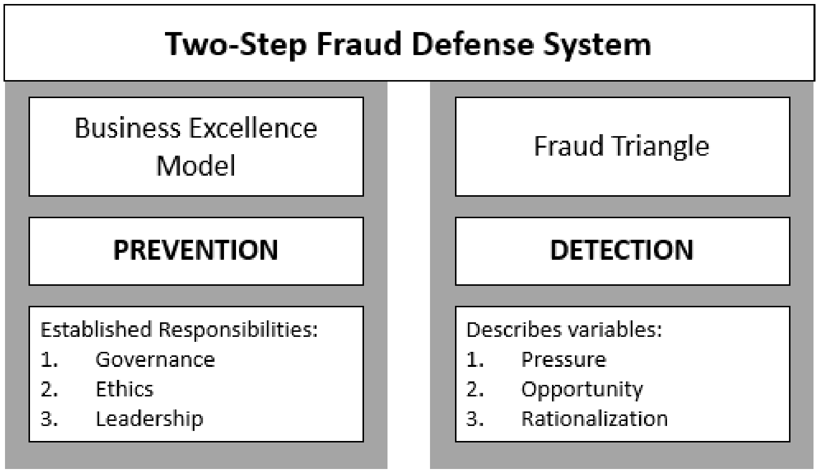

Figure 3. Two-Step Fraud Defense System. Composed by the author according to Riney (2018)

While reviewing various structures, it is noticeable that detection and prevention components were included in all the mentioned approach frameworks. It is also significant to note that the third factor differs across authors, with some incorporating several additional parameters. Baesens, Van Vlasselaer, and Verbeke agree that fraud detection and prevention are essential components of an effective anti-fraud program. Furthermore, the authors emphasize that those two components should be combined and considered as a whole. The capability to recognize or identify fraudulent behavior is referred to as fraud detection. Fraud prevention refers to steps that may be taken to avoid or minimize fraud risk. (Baesens, Van Vlasselaer, Verbeke, 2015).

Not all authors agree with Baesens, Van Vlasselaer, and Verbeke approach, that prevention and detection elements are not independent and should be considered simultaneously. Abdullahi and Mansor emphasize the importance of fraud prevention in the first place. It is stated that investing in fraud prevention rather than detection is more cost efficient. Detecting fraud is time-consuming and expensive, and the odds of recovering the money are significantly slim. Investing in fraud prevention, on the other hand, pays off because it decreases the risk of fraud-related losses (Abdullahi, Mansor, 2015). On the other hand, Bolton and Hand discuss the importance of a fraud detection approach, as fraud prevention does not always succeed. They also observe that a fraud detection strategy is not a fixed process, but rather one that is always developing (Bolton, Hand, 2002).

Three senior fraud professionals, Stamler, Marschdorf, and Possamai, have published a book entitled "Fraud Prevention and Detection: Warning Signs and the Red Flag System," in which they evaluate and demonstrate the relevance of fraud detection by recognizing red flags and abnormalities. Those abnormalities or anomalies and red flags indicate acts that are out of the ordinary, unanticipated, and might be indicative of fraud. The necessity of fraud prevention and the need to safeguard businesses from the harm that may be caused by fraud were two additional topics that got a great deal of attention (Stamler, Marschdorf, Possamai, 2016).

Client behavior, as well as fraudulent behavior, changed as a consequence of the Global Pandemic. COVID-19 accelerated the development of the environment that is beneficial to online fraud. For example, shifting from tangible money, paperwork, and identification to digital. In 2021, the Association of Certified Fraud Examiners, together with Grant Thornton LLP, released a report that includes a detailed analysis of various businesses' adaptations to COVID-19 as well as an assessment of how firms are preparing their strategy for post-pandemic fraud management. The issue being investigated is how businesses will adjust in the post-covid era (The Association of Certified Fraud Examiners, Grant Thornton LCC, 2021). According to the findings of the research, more than half (51%) of organizations have discovered more fraud since the beginning of the pandemic. By 2022, 71 percent of companies and organizations expect the level of fraud in their businesses to increase. 38 percent of organizations have decided to increase their investment in anti-fraud technologies for the year 2021. In response to the pandemic, 80 percent of the organizations surveyed have already implemented one or more adjustments to their anti-fraud programs.

The recent increase in fraud could be supported by PricewaterhouseCoopers’ Global Economic Crime and Fraud Survey 2020. According to the survey, 47 percent of experts have experienced fraud in the last 24 months. Compared to the previous 20 years, this is the second highest result. And this indicates that the recent number of identified fraud incidents is increasing (PricewaterhouseCoopers, 2020). They also uncover two characteristics that have a significant impact on the fraud risk environment. Shifts in company procedures and changing client behavior are examples of this. To make anti-fraud initiatives more effective in the future, experts were asked what improvements needed to be made. Experts highlighted enhanced fraud risk awareness across the organization, increased coordination and collaboration, improved fraud risk assessment process, enhanced fraud risk identification process, and enhanced technology for anti-fraud programs (PricewaterhouseCoopers, 2020).

1.4. Fraud Prevention and Detection Software

The study conducted by Mangala and Kumari brings recommendations for organizations towards the effectiveness of fraud detection and prevention. They emphasize the importance of focusing on building a strong internal corporate control system and implementing appropriate fraud risk management. Additional recommendations for organizations are the use of real-time information technology tools, which will assist in the monitoring and identification of unexpected patterns or abnormalities in corporate data, as well as the detection of prospective fraud attempts (Mangala, Kumari, 2017).

Fraud detection and prevention may be accomplished via the use of a variety of real-time information technology software applications. Ahmed, Ansar, Muckley, Khan, Anjum, and Talha in the article "A Semantic Rule-Based Digital Fraud Detection" reviewed and provided a taxonomy of fraud detection technologies. The methodologies for detecting fraud were given, and they may be categorized as social networking, data mining, nature-inspired, sematic, machine learning, and hybrid. The authors also distinguish between two aspects of digital fraud, which were already mentioned in this work: prevention and detection. According to the authors, prevention should be as effective as a hard stop, whereas detection is concerned with recognizing an attack that has already occurred or is still occurring (Ahmed, Ansar, Muckley, Khan, Anjum, Talha, 2021). Various other authors describe and emphasize the importance for organizations of implementing powerful fraud prevention and detection software as the most important weapon in the fight against fraud (Fang, Li, Zhou, Yan, Jiang, Zhou, 2021), (Louzada, Ara, 2012), (Guo, Chaonian, Hao Wang, Hong-Ning Dai, Shuhan Cheng, Tongsen Wang, 2018).

Standard fraud prevention and identification technologies, as recommended by auditing standards, are constructed using the logical red flags-based approach to fraud detection and prevention (Baader, Krcmar, 2018). The presence of red flags indicates that there has been unexpected or out-of-the-ordinary customer behavior. Anti-fraud software is a tool that can detect fraudulent activity using rules based on red flags. These systems collect information points, process them through a set of rules, and then calculate a fraud risk score for the customer, the transaction, the activity, and so forth. Thresholds are used in systems to restrict the score with a particular response action being performed for each threshold. Typically, response actions delivered by the system are accepted, rejected, or revised (Del Mar Roldán-García, García-Nieto, Aldana-Montes, 2017). This indicates that if a transaction, application, or client activity has a low fraud risk score, it may be approved. After receiving an average score, an action may be challenged with further criteria, such as supplying more data, choosing a different payment method, or manually examining the client application (if applicable). Whenever a client's action is deemed to be at the greatest risk of fraud, the activity is immediately denied.

Data points for anti-fraud software can be collected in accordance with the organization's established process. Typically, this might include data points from the client application, logins, and website actions, mainly because "every user action leaves traces in the system." (Baader, Krcmar, 2018, p. 3). Data points relating to customer identification include IP (Internet Protocol) address intelligence, face recognition, finger recognition, device fingerprinting, behavioral biometrics, or biometric data. These are just a few examples of customer identification data points that could be used in rule-based fraud prevention systems. The fraud rules might be based on several different patterns or red flags. For example, consider the following scenarios: the customer is using an email address that was generated just five minutes before the application was submitted, or the address received from the IP address is different from the address provided in the application. When a pattern is recognized by anti-fraud software, it may be based on a single characteristic, such as the network to which the user is connected.

More sophisticated anti-fraud software can detect robotic behavior (bots), indicating that the application was not filed by a human. Malicious bots can be used for fraudulent activities and various treats (Kolomeets, Chechulin, Kotenko, 2021). Bots are capable of disseminating spam and malware, as well as simulating humans. User behavior events such as mouse movements or keyboard use can offer information that can be used to determine if the user is a human or a bot (Chu, Gianvecchio, Wang, 2018). For existing clients, behavioral data, such as client behavior during application and initial login mismatches with client current behavior, might indicate suspicious event and fraudulent attempt to take over client account (Thonnard, Dabbabi, Mironescu, Fontanes, 2018)

Using a device fingerprinting technique, you may determine the uniqueness of a certain electronic device. For existing customers, this is a standard methodology for identifying fraudulent attempts and alerting them to it. In order to generate the fingerprint of a device, data points such as the geographic location of the device, the browser name and version, the IP address, the operating system name and version, the network ID, the mobile identifying number, the IP address of the router, and so on are gathered. These and many more factors are used to develop a device fingerprinting methodology that may be used to identify the device under consideration. This is comparable to the device's unique signature (Kumar, Gambhir, 2018). Device uniqueness is frequently employed in fraud protection and detection software because it may be used to identify abnormal activity or to determine whether a device has previously been used by another customer.

Bolton and Hand analyzed statistics and machine learning technologies for fraud detection. One of these learning technologies is biometric methods, which identify a client's online behavior. Bolton and Hand also highlight the key issue with those technologies – the effectiveness and speed of fraud recognition. "Measures of this aspect interact with measures of final detection rate: in many situations, an account, telephone, and so forth, will have to be used for several fraudulent transactions before it is detected as fraudulent, so that several false negative classifications will necessarily be made." (Bolton, Hand, 2002, p. 246)

Time is also an essential element since the earlier fraud is discovered, the less loss and damage may be done to the organization. According to the Association of Certified Fraud Examiners, there is a significant correlation between the period length before fraud identification and actual loss (The Association of Certified Fraud Examiners, 2020). A proper fraud management strategy must be developed and implemented in advance to minimize the negative impact of fraud on the company. Mangala and Kumari (2017) in their study also highlight the time which is needed to uncover fraud. The authors emphasize that "the longer the period to uncover fraud, the larger the loss in terms of money, legal cost, and image of the organization. Anti-fraud tools should be used in all types of organizations, irrespective of size and type." (Mangala, Kumari 2017, p. 137)

Guo, Hao, Dai, Cheng, and Wang in 2018 proposed a novel fraud monitoring approach based on a combination of online score rules and an offline machine learning subsystem based on historical client data. This new method was tested for electronic banking transactions. The online part of the scoring model combines transactional behavioral data, risk of activities and data collected during identification. In the offline part, there was a combination of machine learning from historical transactions and random forest algorithms, which were proposed for the learning of fraudulent transactions (Guo, Hao, Dai, Cheng, Wang, 2018).

There is a large supply of anti-fraud software that is available. Puiu in 2014 presented a market review for anti-fraud software and mentioned that there is no "silver bullet" for fraud fighting and that each software has a field in which they work best (Puiu, 2014). Different fraud risks are associated with diverse processes. It is important for every company to assess their processes and identify the phases at which fraud is most likely to occur. As a result, the software should be selected in accordance with the specific organization’s requirements.

On the other hand, an important factor to consider is human resources, which will be using the anti-fraud tool. The Global Economic Crime and Fraud Survey conducted by PricewaterhouseCoopers in 2020 discovers that the anti-fraud tool itself, or technology itself, will not protect fraud. The tool's success depends on the professionals who are using the tool, controlling the tool, and monitoring the activity. According to the same survey, nearly 40% of the companies that are utilizing artificial intelligence technologies to combat fraud are having difficulty determining the true value of these technologies. This clearly demonstrates, once again, that technology is less valuable when there are insufficient human resources or professionals available (PricewaterhouseCoopers, 2020).

1.5. Anti-Fraud Software Implementation Challenges

Organizations have traditionally responded to fraud incidents rather than anticipating them and investing in anti-fraud management strategies, as has been the practice for ages. Consequently, a more proactive and forward-thinking strategy is necessary, and investing in fraud prevention and detection demonstrates the company's commitment to ethical leadership and its culture (Eryanto, 2020). According to the Association of Certified Fraud Examiners, the size of the company is also an important factor in fraud detection and prevention. Small-scale organizations often have less fraud controls than large corporations since they also have fewer internal controls, which makes them more vulnerable to fraud. Larger organizations, on the other hand, have more controls in place. However, those organisations are challenged with the difficulties of bypassing existing security measures and internal controls (The Association of Certified Fraud Examiners, 2020). Additionally, when it comes to project management, the size and leadership of the organization are important considerations to make. A significant number of projects may be overseen by professional project managers, who are capable of successfully finishing them for an organization with a great deal of expertise. On the other hand, an organization that does not consider fraud dangers to be significant will not make the necessary investments in effective project management. It is conceivable for such an organization to have substantial challenges while putting fraud-fighting systems and procedures in place.

One of the most challenging aspects of implementing fraud prevention and detection software its effectiveness is highly dependent on the position of management inside of the organization. Unless senior management provides sufficient support, the project will be assigned a low priority and will struggle to achieve success. The significance of this challenge has been stressed by several different academics.

Eryanto conducted research and identified three fundamental reasons contributing to the failure and ineffectiveness of anti-fraud initiatives in Indonesian public sector institutions. These three factors are illustrated by cultural or ethical standards, political considerations, and ethical leadership. The attempt to recognize someone with strong ethical leadership characteristics who really can persuade the whole business to take anti-fraud measures seriously expresses itself as the form of ethical leadership challenge (Eryanto, 2020).

The ethical leadership is the concept which contains of social responsibility, high ethical standards, transparency, and many other characteristics. Brown, Trevino, and Harrison analyzed ethical leadership from the descriptive perspective. According to them, ethical leadership can be defined as a combination of characteristics and behaviors that include demonstrating integrity and high ethical standards, treating employees with consideration and fairness, holding employees accountable for ethical behavior (Brown, Trevino, Harrison, 2005). Another group of scholars looked at ethical leadership as playing a moderating influence in the area of corporate social responsibility. Furthermore, the elements that were analyzed were from the standpoint of the leaders. For example, leaders may impose penalties on workers who breach ethical norms, make choices, or listen to employees' concerns while they are in charge (Kim, Kim, Kim, 2021).

Several additional authors have underlined the significance of leadership in fraud prevention, detection, and response. Roseline conducted research and concluded that the tone established by senior management is essential in establishing an anti-fraud culture inside organizations. The "tone" addressing fraud that will be followed by the rest of the company is defined by the leadership. On the other hand, managers that do not wish to implement anti-fraud processes in their organizations constitute a considerable risk, which can result in fraud losses (Roseline, 2019). Videnovic and Hanic emphasized the responsibility of leaders to set ethical standards that will influence all stakeholders, including employees, investors, shareholders, customers, and suppliers. Furthermore, when fraud is detected, organizational leaders should gather all relevant authorities to collaborate and coordinate their response to the fraud. (Videnovic, Hanic, 2021). Other studies have emphasized the need for implementing fraud prevention and detection mechanisms with the chief executive officer (CEO) and board of directors taking an active role and fully supporting them. Furthermore, anti-fraud measures have a decreased possibility of being successful in their intended purpose if senior management does not support and promote an anti-fraud culture (Hashim, Salleh, Shuhaimi, Ismail, 2020).

Previous writers were agreed upon by Bartsiotas and Achamkulangare: "The leadership and commitment of the executive head and senior management are essential to combating fraud by setting the example for ethical conduct and creating an anti-fraud culture throughout the organization." (Bartsiotas, Achamkulangare, 2016, p. 5). A leadership perspective from the standpoint of an anti-fraud leader was also studied by the authors. They put forward the recommendation for organizations, which describes the importance of delegating "a senior person or team as the "business process owner" of all fraud-related activities" (Bartsiotas, Achamkulangare, 2016, p. 5). As part of his or her duties, this delegate would be responsible for monitoring and reporting on fraud-related activity inside the organization. The same person or team should be held accountable for implementing and monitoring the anti-fraud policy. Meinert similarly emphasized the significance of appointing an anti-fraud professional. She published an article in which she emphasized the necessity of corporations hiring the strongest anti-fraud professionals. The justification for its importance is that a competent anti-fraud expert with strong leadership competences will bring together numerous departments and encourage them to work together in the correct direction, which will benefit everyone. (Meinert, 2016).

Another group of challenges which might affect successful anti-fraud software implementation are technical challenges**.** Complexity is one of those technological challenges. Kurshan and Shen discovered that traditional rule-based anti-fraud systems have become ineffective in recent years, as digital payments, crime typologies, and channels have grown. They researched the use of graph methods in conjunction with artificial intelligence as an alternative future option, as well as the potential challenges of implementing such techniques. The major challenges are the size, speed, complexity, and adversarial characteristics, "the large-scale implementation requirements, real-time processing, siloed nature of the channels, frequent updates, and complex data/graphs make the deployments and reaching the detection performance targets difficult" (Kurshan, Shen, 2021, p. 20). Data security requirements also add to the complexity of anti-fraud software implementation. Sensitive user data must be protected and encrypted in order to be secure. (Jianhao, 2019).

However, even though complexity brings challenges during anti-fraud software implementation, it cannot be overridden. Complexity and dynamics are required components of anti-fraud solutions. In this circumstance, fraud detection and prevention measures cannot be simple and static because fraudsters may simply bypass them. At that time, the fraudster knows the principle of anti-fraud software: it becomes ineffective when the fraudster adapts it to their strategy. Detection of fraud must be continuously updated. (Bolton, Hand, 2002). Furthermore, fraud detection should be adaptable and capable of detecting developing fraudulent patterns. Fraudsters are seeking the most inventive ways to commit fraud, so anti-fraud software must include machine learning models that are flexible and capable of identifying new patterns.

Every organization may choose the software that is most comparable to or performs the best for their operations from among many options accessible (Puiu, 2014). Nevertheless, the software should operate in various environments, and according to Orso, "software can behave very differently in different environments and configurations. It is difficult to assess its quality purely in-house, outside the actual time and context in which it executes" (Orso, 2010, p. 263). Additional in-house testing, according to this point of view, should be considered before going live to limit the possibility of underperformance.

Nevertheless, anti-fraud technologies do not make this as straightforward as it seems. Fraud detection results may be used to assess the overall quality of anti-fraud software by evaluating their precision. There are four categories of outcomes that may be obtained: true positives, false positives, true negatives, and false negatives. True positives demonstrate fraud that has been appropriately identified. False positives are instances of fraud that were mistakenly recognized. True negatives are actions or transactions that have been accurately determined as non-fraudulent. False negatives are transactions or activities that have been mistakenly identified as not fraudulent (Bobinas, 2018). False negatives and false positives are the characteristics of anti-fraud software that cause it to perform below expectations. While there is no such thing as a 100 percent accurate prediction of fraud, it is conceivable that a part of the transactions, activities, or behaviors being tracked may be flagged as fraudulent by mistake. And this portion is disproportionately large (Beneish, Vorst, 2021). It has been highlighted by some researchers that false positives may cost some organizations as much money as actual fraud in terms of lost revenue (Wedge, Kanter, Rubio, Perez, Veeramachaneni, 2017).

1.6. Project Management Success Model

The implementation of anti-fraud software should be approached in the same approach as any other project, with the same fundamental project success criteria in mind. Successful project management characteristics are a broadly discussed topic among various authors. There is no single accepted theory that defines the fixed variables required for successful project management. Similarly, to the Fraud Triangle Theory, project success may be stated in essence by combining tree components. When it comes to project management success, the Iron Triangle symbolizes the interaction of three factors: time, cost, and quality (Neverauskas, Bakinaite, Meiliene, 2013). However, much as the Fraud Triangle theory was criticized and other parameters were recommended, critics of the Iron Triangle have encouraged that additional factor to be considered. Prostejovska and Tomankova classified the supplementary variables into three categories: stakeholders, context, and management. The authors also highlighted that the success of a project is heavily influenced by a group of stakeholders' criteria (Prostejovska, Tomankova, 2017). Other authors state, that

Iron Triangle gives "only a hefty imagination of project success" (Neverauskas, Bakinaite, Meiliene, 2013. p. 835). According to the same authors, the Iron Triangle lacks internal and external communication, stakeholders, and project environmental conditions.

Using the Triple Constructs, which was developed by Mulcahy, you may assess the success of a project by looking at the following factors: timing, cost, scope, quality, risk, and customer satisfaction. To ensure a successful project, it is necessary to maintain a proper balance between all the project's components. Aside from that, Mulcahy describes the art of project management and outlines a variety of skills that are included in the art of project management such as negotiating, resolving conflicts, giving feedback, building a team, and so on. Mulcahy also discusses the importance of communication in project management (Mulcahy, 2006).

Bullen and Rockart published "A Primer on Critical Success Factors" in 1981, in which they introduced the concept of critical success factors and stated that "the key to success for most managers is to focus their most limited resource (their time) on those things which really make the difference between success and failure." (Rockart, Bullen 1981, p. 12).

Discenza and Forman have identified and summarized several important project management functions that are necessary for effective project management. In comparison to earlier writers, Discenza and Forman add efficient and effective communication abilities, as well as appropriate technical and non-technical resources (Discenza, Forman 2007). The same importance of communication was also emphasized by other authors Durmic (2020) and Yong, Nur (2017). Later, Yong and Nur investigated those important success components in further depth, emphasizing the importance of stakeholders' attitudes and behaviours in determining project success. The relevance of human factors in project performance was emphasized by the authors. (Yong, Nur, 2017).

The importance of communication within the project team was also one of the outcomes from the study accomplished by Durmic (2020). The research defines information technology project performance and outcomes as success factors. It was indicated that "project team and project control components have the highest influence on the project's success, while project planning has a medium impact" (Durmic, 2020, p. 1019). This study also provides guidelines for organizations based on project management, and one of the main recommendations is an investment in people, their collaboration, and their knowledge base. Employees that have more expertise are much more capable of forming stronger teams, which may result in the success of projects in the future. It is in this perspective that the Project Management Institute’s research makes a significant contribution by identifying the most significant attributes that lead to project failure. In 2017, the most significant factor was "a lack of clearly defined and/or achievable milestones and objectives to measure progress," which was followed by "poor communication" and "a lack of communication by senior management," according to the Project Management Institute (Project Management Institute, 2017, p. 11).

Particularly, Van Der Westhuizen and Fitzgerald focused their attention on the elements that contribute to the success of software projects in particular. A conceptual model was developed by the authors, which demonstrated that project success equals the total of the project management and product success components. In order to be considered successful, project management had to meet three criteria: it had to be completed on time, under budget, and in accordance with requirements. The previously mentioned triple constructs model, which takes into account time, budget, and quality, is nearly identical to the model described here. Van Der Westhuizen and Fitzgerald expanded their list of three primary criteria to include the fulfillment of project stakeholders' expectations as well as the overall quality of the project management process.

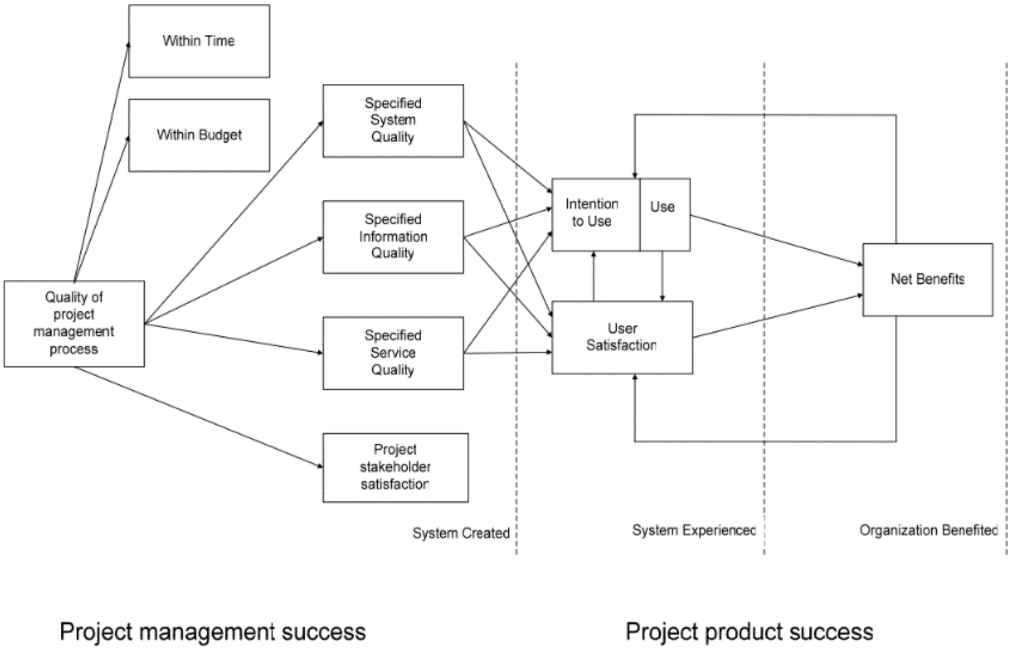

Figure 4. A More Comprehensive Model for Project Success. (Source: Van Der Westhuizen & Fitzgerald 2005, p.13)

The DeLone and McLean model of information system success was used in order to determine the components that contribute to product success. This fundamental model has been developed as a consequence of an empirical and theoretical investigation. The six components of this framework are as follows: system quality, information quality, information utilization, user happiness, individual impact, and organizational effect. Van Der Westhuizen and Fitzgerald established a conceptual model for software project success that was based on a modified version of DeLone and McLean's methodology, as seen in figure 4.

Despite the fact that Van Der Westhuizen and Fitzgerald's models were first introduced in 2005, they are still relevant and may be employed for software implementation projects. There are several critical components missing from the model, however. These are components, such as leadership and communication, that are increasingly being added in new models and emphasized by other writers (Discenza, Forman, Durmic, Yong, Nur).

Even more recent research, done by Guo (2019), discovered that the success of an information system project can be predicted using a model that contains three constructs: the success of the project management, the outcomes of the project, and contextual factors. The idea of this concept was “project management success alone cannot guarantee project success; project outputs and contextual factors also influence success through the leadership of the project manager throughout the lifecycle.” (Guo, 2019, p. 53). Guo pointed out that only a minority of all information technology projects were finished within conventional project success factors (time, cost, and quality), which address project efficiency. It is noted by the author that paying too little attention to project outcomes results in "many unexplainable project failures" (Guo, 2019, p. 57). This model also highlighted the importance of involvement of software users

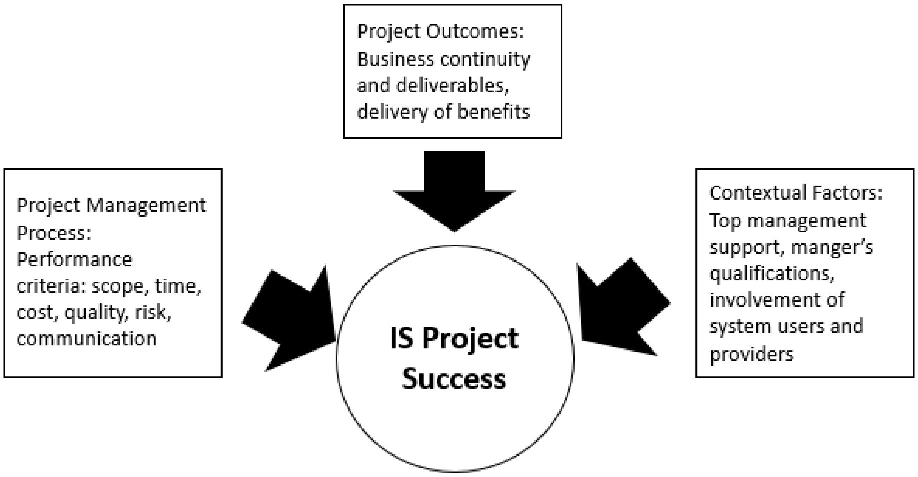
Project Outcomes: Business continuity and deliverables, delivery of benefits
Project Management Process: Performance criteria: scope, time, cost, quality, risk, communication
Contextual Factors: Top management support, manger’s qualifications, involvement of system users and providers
IS Project Success

Figure 5. Information System (IS) Project success model. Composed by the author according to Guo (2019)

and providers. In anti-fraud software implementation project this would refer to the involvement of fraud team and anti-fraud software providers.

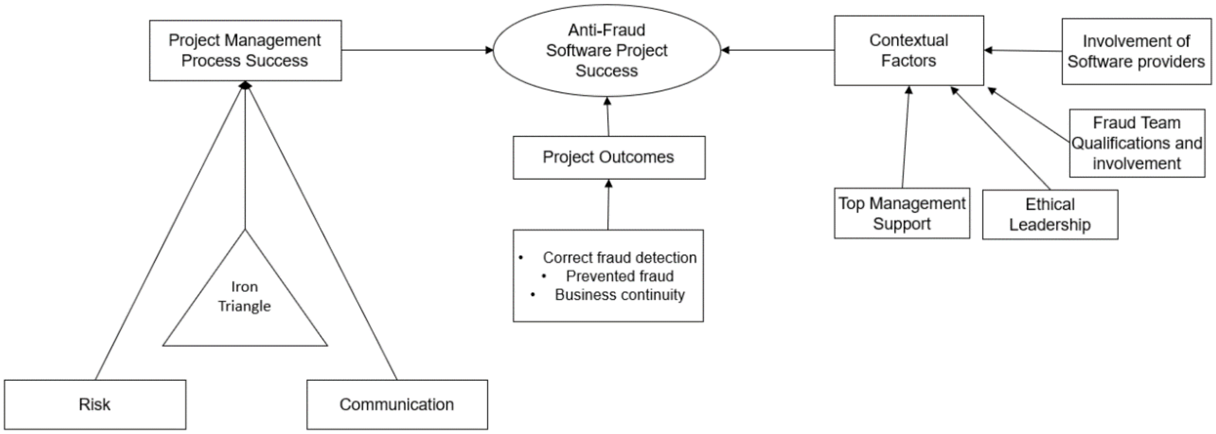

Figure 6. The Conceptual Anti-Fraud Software Implementation Project Success Model. Composed by the author (2021)

The conceptual model for anti-fraud software implementation project success was created by combining several conceptual information system project success models, various project success variables, and the difficulties and particularities of anti-fraud projects which arrived from the literature review. The model of three constructs proposed by Guo was used as the fundamental model (figure 5). Nevertheless, each construct included the specifics arrived from the literature review. The conceptual anti-fraud software implementation project success model (figure 6) contains three constructs:

- The success of the project management process, which is founded on the Iron Triangle principles of cost, time, and quality, is the first construct to consider. These variables cannot be disregarded since they are critical to the success of the project. Additional elements were also addressed, including communication and risk assessment. Risk assessment refers to the detection of anti-fraud software complexity, dynamism, and the fact that software might operate quite differently in various companies. Effective communication is another critical element that has been noted by a number of authors and should be considered as the construct on the success of the project management process.
- The second component is defined as project outcomes, and it corresponds to the continuity of business operations, the production of deliverables, and the obtaining of benefits. A strong indication of fraud, along with a decreased likelihood of false negatives, is critical in an anti-fraud technology. The technology should also provide data with less biases. The quality of

project output is dependent on the organization's processes and systems, which will be incorporated with anti-fraud software.

- The last construct consists of contextual factors that outweigh the relevance of a leadership position and top management commitment for an anti-fraud culture in the organization. The high-quality anti-fraud experts' team, which will be the primary users, and who should be able to appropriately pick the tool that is most appropriate for the organization's demands, or simply convey the requirements for an anti-fraud program, is also important. Another important consideration is the level of customer service given by the anti-fraud software provider.

The conceptual model for anti-fraud software implementation project success represents the main specifics of anti-fraud software projects formulated from the literature review. The constructs from the conceptual model (figure 6) will be examined during the following research.

2. ANTI-FRAUD TECHNOLOGY RESEARCH METHODOLOGY

2.1. Empirical Approach to the Research and Research Questions

According to the objectives of this master's thesis, it was necessary to perform an assessment of anti-fraud software implementation projects in order to identify the most significant principles for the effective completion of such projects. The initial part of the investigation consisted of conducting a thorough examination of the scientific literature. A review of scientific literature resulted in factors that have an impact on anti-fraud software project selection and the development of a conceptual model that outlines the most significant success criteria for anti-fraud software implementation projects. However, the successful completion of the anti-fraud software implementation project may be dependent on a number of other components that were not addressed throughout the literature research.

The contextual factors (top management support, involvement of software providers, ethical leadership, fraud team qualifications, and involvement) were preferred as the major research considerations. Therefore, contextual factors' relationships with successful project management for anti-fraud software implementation will be analyzed in further research. In addition to this, the empirical research phase will contribute to the identification, description, and classification of the specifics of anti-fraud projects.

The empirical research continued with an additional objective: a comparison of theoretical and practical outcomes. The perspectives of professionals with previous experience in anti-fraud software implementation projects were gathered to produce practical implications for the research. This was accomplished using qualitative research and expert interviews. Because it was essential to collect comprehensive and specific replies from experts, qualitative research was chosen.

Because this field of research is relatively new in terms of research, it is necessary to acquire essential information from experts in that subject. Using this research methodology, it was attempted to avoid obtaining biased responses. Consequently, a standardized open-ended interview with experts who are now working on or have previously worked on anti-fraud software implementation projects were conducted. During the interview, experts were asked to provide a wide range of responses to open-ended questions that have tested and have demonstrated their opinions and experience on specific categories of topics. The literature research contributed to underlining the topic's importance and developing interview subjects and questions.

The sample of experts was selected according to the criterion sampling method (Rupšienė, 2007). There are clear requirements for the interview participants. The experts must have work experience with anti-fraud software implementation projects. The experts for the interview were selected according to their experience in working with anti-fraud software implementation projects. The first group of participants were acquainted with the author and were approached personally. Other part was approached via the professional social media channel LinkedIn, targeting professionals with the required experience. A snowball sampling strategy was used to choose the remaining participants based on expert recommendations. In this methodology, experts provided advice and nominated professionals who they considered would be valuable to the research.

The interview was conducted in absolute confidence and anonymity, and the experts were informed that the information they provided would only be used for this specific master's thesis paper, which they gladly obliged to. The interview questions were standardized to eliminate the chance of prejudice on the part of either the interviewer or the interviewee, as well as data biases. The interview was conducted, and the data collected online, which helped to maintain the anonymity and confidentiality of the subject matter experts.

The interview questions were divided into three groups:

1) The initial group of questions collects general information about the expert and should represent his or her individual experience with anti-fraud implementation projects, their function in the project, and general experience with implementation projects. This information assisted in the apportionment of findings depending on specific expert characteristics.
2) The following group of questions requires the interviewee to select one of the anti-fraud software implementation projects in which he or she was involved and evaluate his or her individual perspective on the project's characteristics. These characteristics include the project's success, the difficulties experienced during the project, senior management engagement and support throughout the project, the fraud team's qualifications and involvement, and the software provider's commitment. These responses aided in establishing relationships between contextual variables and project performance. Additionally, this part's findings resulted in the definition of anti-fraud software implementation project specifications.
3) The final section of the questions asked experts for professional opinions and wide-ranging perspectives on topics such as: what are the most likely causes of anti-fraud software implementation difficulties or delays, and what are the most important takeaways or lessons learned from those projects, to name a few examples. Additionally, experts were asked to provide professional advice to project managers in charge of anti-fraud software installation

projects. This portion of the interview will go further into the expert's past experiences and may reveal areas of the research that were not covered during the theoretical phase of the study.

A total of twelve experts were approached and interviewed for the purpose of this research. The experience of the professionals questioned were ranged into three groups – less than 6 years, from 6 to 10 years and from 11 to 15 years. The majority of the experts who participated in the research had between 6 and 10 years of expertise in their respective fields. The responsibilities of experts varied significantly between projects and include fraud managers, business analysts, software architects, software testers, fraud analysts, project managers, and specialists. The fact that all the experts were involved in anti-fraud software implementation projects was the underlying factor that tied them all together.

The findings of the investigation were arranged and evaluated in accordance with a systemic approach. Each question constituted a study category, which was then thoroughly investigated. To organize the responses from the experts, responses were divided into subcategories that reflected difficulties encountered, project success evaluations, or other specifications regarding anti-fraud software implementation projects. Expert replies were compared to their own previous responses as well as responses from other experts to better understand the specific conditions and influences on responses. Furthermore, by examining subcategories, it was possible to obtain a more comprehensive picture of all the specialists and expert groups.

2.2. Presentation of the Research Participants

The first batch of interview questions is designed to elicit general information about the experts and should reflect their individual experiences with Anti-Fraud implementation projects, their roles in the projects, and their overall experience with software implementation projects. The years of experience of an expert, as well as their position within their organization's fraud-related initiatives, were summarized in table 1.

Table 1. Interview Experts Experience and Roles

Expert	**Experience**	**Role in the project**
Expert 1	6-10 years	Fraud Manager
Expert 2	6-10 years	Business Analyst/Product Owner
Expert 3	6-10 years	Software Developer - Testing
Expert 4	6-10 years	Fraud Prevention Analyst
Expert 5	11-15 years	Software Architect, Lead Engineer (Software provider)

Expert 6	11-15 years	Project Leader
Expert 7	6-10 years	AML Compliance Expert
Expert 8	0-5 years	Specialist (Fraud team)
Expert 9	6-10 years	Project Manager
Expert 10	0-5 years	Specialist (Software provider)
Expert 11	6-10 years	IT Support (Software provider)
Expert 12	6-10 years	Fraud Manager

Source: Composed by author

The experience of experts is classified into three categories based on their age range: less than six years, six to ten years, and eleven to fifteen years. The significant majority of replies (8 out of 12) indicate a tenure of between six and ten years. Two interviewees belong to the group of workers who have been working for less than six years. Two participants are included in the group with the most years of proven experience.

Fraud managers, business analysts, software architects, software testers, fraud analysts, project managers, and specialists are among the positions represented by the experts who took part in the interview. Positions can also be classified into a few distinct categories.

These are the primary users or clients of anti-fraud technology, which includes fraud specialists, compliance experts and fraud analysts, who fall into the first of these categories. Fraud analysts and specialists often have less experience of project management process, but they are certainly specialists in their respective field. Their work during project is focused on developing specifications for the tool and exchanging samples of fraudulent circumstances that should be recognized by the software. They are taking part in the tool's testing process and can provide feedback on tool performance.

Other category of experts are employees with the senior position in fraud management. These employees are fraud managers or risk managers, who not necessarily will use the tool directly, but who are heavily involved and accountable for the tool's implementation within the organization. In small organizations, with no project manager positions, fraud managers are responsible for managing the anti-fraud software implementation projects from beginning to end.

Project professionals, which include project managers and product owners, make up the third category of experts. These individuals represent larger organizations that already have established project management processes and the resources to delegate project managers to oversee such a project. Small businesses appoint fraud managers or information technology managers to handle anti-fraud software implementation projects.

The last category of interviewees consists of information technology professionals, including software architects, software testers, and specialists. This group might alternatively be divided into two subcategories: those who work as specialists within the organization and those who work as software vendors. Three experts from three separate anti-fraud software companies were interviewed for this research.

3. RESEARCH OF ANTI-FRAUD SOFTWARE FINDINGS AND DISCUSSIONS

3.1. Anti-Fraud Software Implementation Projects Uniqueness

The first category of qualitative research which was analyzed, was anti-fraud software implementation projects uniqueness comparing with conventional projects. Interviewed experts' experience working on previous software implementation projects differs significantly according to their job title or professional background. Experts who were working in fraud roles or were specialists have significantly less expertise with other software implementation projects. And, in most cases, the projects in which they were participating were connected to fraud detection and prevention programs. On the other hand, information technology specialists and project managers have extensive expertise with a variety of projects and positions within those projects. Additionally, professionals with more broad expertise may also examine and find distinctions between anti-fraud software implementation projects and other non-fraud related projects.

The majority of experts' responses resulted in the formation of a “compliance with legal requirements” subcategory. The most common criteria which differs anti-fraud project from regular project are legal, regulatory and security requirements. In some ways, fraud detection is a sensitive topic because the algorithms are based on a large number of personal datapoints. On the one hand, it complicates implementation. But at the other side, internal and external audits result in important findings and suggestions for organizations on how to detect and prevent fraud, which also results in rather stringent standards for the tool that will be utilized in the organization. According to the expert 5, legal requirements are more stringent for projects involving fraud detection and prevention than they are for other types of software implementation projects that are not related to fraud. Expert 7 acknowledged the need of having legal experience at the expert level throughout the project's duration. Expert 2 emphasized the importance of the involvement of the compliance department. Because of the large number of legal criteria that needed to be met, this was one of the most important departments.

Another commonly mentioned characteristic resulted in formation of “complexity and diversity” subcategory. During fraud software implementation project team should adapt project to “today's needs and to look forward to a rapidly changing environment” (expert 3). The reality is that requirements for the tool can change even during the implementation, and it is difficult to establish the appropriate scope in the beginning on planning phase. Another criterion of complexity is the amount of different fraud scenarios that must be identified and prevented. According to the expert 3, the implementation team should consider a large number of aspects to guarantee that anti-fraud software will be a strong instrument or that the global features of fraud will be addressed. Experts 7 and 6 acknowledged that a greater number of teams involved with the project was one of the characteristics of complexity that needed to be considered.

Among the qualities highlighted by the expert 3 are those that may be classed as belonging to the subcategory of "creating trust across organizations." In the opinion of the expert, anti-fraud software implementation projects help to strengthen the company from the inside out, which in turn helps to develop confidence and prevent the occurrence of fraud. Expert 4 has discovered that anti-fraud related projects are significantly more transparent when compared to other types of projects. As the expert 11 pointed out, anti-fraud software projects differ from other non-fraud software projects in that they require a greater level of participation from the teams that will be using the product. Interviewee 6 agreed, that fraud related projects require more teams to be involved. Those responses were classified as belonging to the subcategory of "organizational engagement".

Expert 12 underlined that the implementation of anti-fraud software projects requires the acquisition of certain skills and expertise by the staff involved in the project. In agreement with that approach, expert 10 stated that it is important to understand how fraud occurs, fraud types, and exceptions in order to successfully proceed with the project. Those answers result in formation of the subcategory of “fraud knowledge”.

The last set of factors identified by the experts is listed below under the subcategory "data specifics". In response to the question, two interviewees indicated data security characteristics such as confidentiality as a feature that distinguishes anti-fraud projects from other non-fraud related projects. Expert 9 stated that anti-fraud projects need an increased level of carefulness when it comes to data since it has the potential to be misused or misinterpreted.

One expert was unable to compare anti-fraud software implementation projects with other types of implementation projects due to a lack of experience and knowledge regard other fields. Another interviewee mentioned an anti-fraud software implementation effort that was comparable to previous software implementation projects. According to this expert, who represents the software supplier's point of view, there were no significant differences between conventional non-fraud related projects and fraud-related projects.

Summarizing experts' responses regarding anti-fraud software project uniqueness comparing with conventional projects there were several subcategories identified and presented in the table 2. Legal requirements and project complexity or diversity, according to the experts, are the most important differences, as shown by the fact that the most widely endorsed subcategories were "compliance with legal requirements" and "complexity and variety the other differences were divided into subcategories, which include “fraud knowledge”, "organizational engagement", “data specifics” and "creating trust across organizations".

Table 2. Anti-Fraud Projects Uniqueness Comparing with Other Projects

Category	**Subcategory**	**Interview statement**
Anti-Fraud Projects Uniqueness Comparing with Other Projects	*Fraud knowledge*	*<…> because every fraud type, even place, where fraud is issued, have many exceptions.*
		This project requires certain fraud skills <…>
	Compliance with legal requirements	*<…> expert level legal knowledge was compulsory <…>*
		<…>more safety as security restrictions <…>
		<…> different regulatory environment.
		The requirements are stricter. Mistakes in software design or simple bugs might cause legal troubles.
		The tool has many legal requirements, which should be fulfilled. And one of the key departments was compliance team.
		The legal framework <…> forced us to adapt projects to today's needs <…>.
	Organizational engagement	*<…>The increased involvement of the people who are receiving the anti-fraud software*
		More teams are involved than usually.
	Creating trust across organizations	*<…>it builds organisation from inside also it helps to build trust prevent the threats <…>*
		Anti-fraud projects are way more open-ended than "conventional" projects.
	Complexity and diversity	*<…> It seemed to be more complex <…> and many teams were involved*
		<…> global features of fraud, forced us to adapt projects to today's needs and to look forward to a rapidly changing environment.
		<…> the tool is complicated.
		The higher frequency of facing unexpected new variables.
		<…>I think that fraud projects have more details, since it includes and tracks a lot of different systems and client actions. It can be more complicated <…>
		<…> the processes that are carried with principle - here and now, as well as that the project and tool itself can change even in the course of implementation <…>
	Data specifics	*<…> As well as it is using sensitive data and should be carried out with high confidentiality.*

		Data security and relatability.
		It helps identify various ways how to misuse data and where to be careful.

Source: Composed by the author

3.2. Selecting Anti-Fraud Software

The following group of questions required experts to choose one particular anti-fraud software implementation project and answer to the questions based on experience during that project. First category in this group discussed the tool selection phase which is one of the most important phases of the anti-fraud software implementation project. This phase might be handled as an independent project or can be integrated as a part of the overall project scope. In any case, it is critical to select the correct tool that will provide the maximum value to the company.

Experts that were interviewed emphasized three subcategories of answers or the most commonly used approaches for selecting the proper tool. Those subcategories are “market research”, “software testing” and “combination of market research and software testing”. Table 3 contains a list of the subcategories as well as the remarks extracted from the experts’ statements.

Seven experts admitted market research, which involves an evaluation of several tools. The tool was then chosen based on criteria such as benefits or disadvantages, pricing, quality, functionalities, or ability to meet the company's requirements. Expert 3 highlights, that their company were targeting “the highest quality tool on the market”. Expert 11 highlights, that the tool in his organization was selected based on price and company use case. Expert 2 answered that tool selection was based on strict requirement which requires to the tool have certain level of security.

Software testing is another option that may be pursued after conducting market research. Before the implementation project, software testing might be a separate project or activity. Furthermore, software testing might be incorporated into the project scope. It is essential to note that if the findings are not satisfactory, the software shouldn't be installed.

Different techniques of testing the ani-fraud software may be used to evaluate its functionality. The first is accomplished by incorporating the software provider application programming interface (API) call into company systems that must be monitored. This method will track real-time data and is the most effective approach to evaluate and challenge the technology. It does, however, need the same input as the conventional implementation project. Which is a favorable thought, because if the tool is selected, it will not require or take just minimal work. However, if the software's outcomes are unsatisfactory, a significant amount of effort will be spent only on testing. Retrospective analysis is another, simpler method of testing. This occurs when a company provides historical logs of its clients' activity to a software provider, who inputs this data to their tool to evaluate how the software will handle such data. Typically, software providers respond with results of transactions or other logs that have been flagged as fraudulent. Because this testing is based on historical data, fraudulent logs or transactions could be included in the sample. As a result, the customer or company evaluating the software could very well compare the results from the supplier to actual fraud statistics.

Some experts stated that during their project, there was a mixed approach to the two most frequent methods of picking the tool: market research and software testing. This approach demonstrates that the organization placed a high importance on the selection of software that is the most appropriate for the organization's business requirements.

Another point that was critical to comprehend was whether tool selection should be included in the scope of the project or should be done independently. The recommendations of the experts were homogeneous in this case since the tool had already been selected in all the projects in which they were involved and was not included in the project scope. There have been some responders who had taken part in a different tool testing project, as well. Because it was tested through integration and needed resources comparable to those required for conventional implementation, a separate project was required. Another expert stated that the software had already been picked by the company and had been supplied for use throughout the project's implementation.

Table 3. The selection of anti-fraud software

Category	***Subcategory***	***Interview statement***
The selection of anti-fraud software	*Market research*	*There was market analysis and research <…>*
		By comparing several existing tools, their advantages, and disadvantages
		Through market research
		Organization was simply interested in highest quality tool on the market, so that was top priority for choosing particular tools
		It was based on FSA requirements to have particular level of security and knowledge about the customers.
	Software testing	*<…> it was in-house testing phase<…>*
		First, they tried to test the given project and match the result with the previous data <…>
		Trial periods
		It was tested, then released <…>

	Combination of market research and software testing	*I was reviewing couple of tools <…> decided to test one of those. <…>*
		The tool was selected based on price and tested on the company use case.

Source: Composed by the author

3.3. The Project Success and The Factors That May Contribute to It

Interviewees' assessments of the success of the project in which they were involved are represented by the project success category. This category is significant for the following categories because it will provide the opportunity to examine the influence of contextual variables on project success based on the responses provided. Experts were asked how they would determine the success of a project and what characteristics they believe make a project successful in their perspective.

Only three experts considered their chosen projects as either unsuccessful or having only limited success. The most often mentioned reasons were a lack of resources throughout the implementation, shifting priorities, changing project managers, and unsatisfactory results. Nine experts considered the chosen anti-fraud software implementation project to be successful. The demonstration of this is that the requirements were fulfilled, and the software was delivered on schedule and in excellent quality. In addition, experts pointed out that the software itself was convenient to use and that the results were satisfactory.

Since success of the project is frequently discussed subject among researchers and could be interpreted differently, there was a question which required experts to describe, what in their opinion characterizes an anti-fraud software implementation project as successful or not successful. A variety of different replies were generated, which resulted in five separate subcategories, which are displayed in the following table 4.

Table 4. The Anti-Fraud Project Success Factors

Category	***Subcategory***	***Interview statement***
The anti-fraud project success factors	*Technical software performance*	*Implementation was great success, because tool was quite easy to handle*
		Really successful, everyday tasks are completed faster, more processes were automated, but several updates after implementation were still needed
	Ability to detect fraud	*If the tool is functioning and catches fraud. Less false positives. More true positives. The prevented fraud losses should be higher than the spending on the tool. <…>*

		project is successful when it's reduces the risk of fraud and also prevent the financial loss.
		<...> and having a never-ending backlog of fraud scenarios to handle.
	Traditional project success criteria	*If set goals are reached, then project is successful.*
		Meeting all the initially planned and subsequently added goals and objectives.
		<...>software was built on time with good quality.
		If it fulfils the present goals
		project delivers the value, stakeholders' satisfaction, and overall satisfying results.
	Compliance with legal and audit requirements	*The project was successful as the company managed to comply with requirements<...>*
		<...>And also, it should comply with legal/audit requirements.
	Feedback from the users	*In my opinion, the most important thing to understand that the project was successful are quick feedback from colleagues <...>*
		Mostly by reviews of everyday users

Source: Composed by the author

There was a group of experts who considered that the success of an anti-fraud project was completely dependent on the performance of the software. Those experts highlighted the convenience with which the technology may be used, as well as the opportunity to automate the process through the use of software. "Technical software performance" is a subcategory of replies that includes those that were provided.

Other experts highlight the traditional project success criteria, like meeting the project scope with high quality, stakeholders' satisfaction, or within time and budget. Those criteria rely on the Triple Constructs approach described by Mulcahy and mentioned in the literature research part of this master's thesis. Expert 12 emphasized that a project should be considered successful if it provides value to the stakeholders and the overall results and outcomes are satisfactory to them. Other groups of experts were close to that by highlighting the importance of reaching the goals and objections settled at the beginning of the implementation or added subsequently. All those responses fall under the subcategory "traditional project success criteria".

Two experts stated that the feedback received from the primary and everyday users of the anti-fraud tool should be used to determine whether or not the implementation project was a success or a failure. This results in the creation of a new subcategory entitled "feedback from the users." The other two experts pointed out that in order to consider a project successful, it must be completed in accordance with legal or audit standards at the conclusion of the project. All the replies fall under the subcategory of "compliance with legal and audit requirements".

After conducting an assessment of anti-fraud project success criteria, the last subcategory discovered was "ability to detect fraud." This was the last subcategory to be identified. Three experts stated that the prevention of fraud losses is an essential element to consider as well. The expert 1 believes that the project will be considered successful if the tool helps to reduce fraud losses and the amount of fraud losses that are averted is higher than the amount of money that was spent on the software implementation. As expert 4 pointed out, the adoption of anti-fraud software is effective when the end result lowers the risk of fraud and protects the business from the financial losses caused by fraud.

To summarize, each expert has their own point of view on what constitutes a successful project's outcomes. And this is influenced by the positions that were carried during the project's lifetime. Fraud experts measure project performance based on the satisfaction of stakeholders, including the identified fraud numbers, the quality of triggered alerts, the functionality of the tool, and the ability of the software to detect fraudulent transactions in the actual world. The fraud managers or experts who own the tool are searching for compliance with legal requirements or a paid back rate – if the loss averted by using the instrument outweighs the cost of the tool's acquisition and maintenance. Traditional project performance measures, such as completing the project's initial goals and objectives or completing project within time and on budget, are used by project managers to determine the success of their projects. Service providers believe that the software's functionality and performance are the primary and only criteria that can be used to determine whether or not it is a success. At the same time, information technology experts from the organization that is implementing the software measure success based on the feedback from the main users and technical performance indicators of the tool.

3.4. Top Management Support

During literature research, several authors emphasized the importance of organization leadership commitment, as well as their attitude towards the subject of fraud. Therefore, one of the contextual factors that was established in the conceptual model was top management support for the project. The fact that this category was incorporated into the initial conceptual model emphasized the need to examine it in the empirical research. Additionally, it is essential to evaluate top management commitment's impact on project success. Experts were asked to evaluate their organizations' senior management's overall commitment and attention to the anti-fraud software implementation project.

According to the responses of experts to the question "How would you evaluate the success of the project?", the great majority of projects were successful, or at the very least were considered successful from the experts' perspective. The majority of experts who rated their project as successful also stated that the project's overall senior management had strong commitment and showed attention to the project's requirements. Interviewees were asked if they agreed that the project was a high priority for the organization that implemented the anti-fraud system in the following question. And all the same experts responded that the project was considered to be a high priority for the organization.

On the other hand, two experts who concluded that the project was either unsuccessful or had limited success also stated that senior management had only permanent commitment and showed minimal attention to the project. Furthermore, in response to the next question on the project's prioritization, they both acknowledged that this project did not appear to be a high priority for the organization. Organization and leadership positions on the project, which was ultimately unsuccessful, were clearly outlined to expert 5. He explained that the project was first given a high priority, but after some time, it became convenient for management - they shifted priorities. Following that, the project was transferred to the backlog of the department of information technology.

There were two experts whose conclusions were completely contradictory. One expert considered the project successful since it achieved its objectives while at the same time demonstrating a lack of commitment from the company's top management. The expert on the other hand stated that fraud analysts were more involved in the project and made a significant contribution to its success. The project was considered failed by the most recent expert, and there was no meaningful remark on senior management commitment at the same time as well. Furthermore, when asked about prioritizing, the answer was "mostly yes," which, when compared to the replies of other experts, appears to be a weak response that does not indicate top management commitment. In any case, neither of the experts who are questioning the relationship provided a definitive and unambiguous response to their questions. There were additional conditions, for example if the project was successful, and there was minimal commitment from the leadership – the additional factor was included to the answer, which might explain why project ended up successfully.

Furthermore, the interviewee 2 highlighted important parameter which might significantly affect organization priorities and top management commitment for anti-fraud software implementation projects. This parameter which accelerates anti-fraud programs in financial institutions is audit findings and warnings regarding noncompliance with legal requirements. There are clear consequences for not being compliant with regulatory and legal requirements. Those consequences might be financial, like regulatory fines, risk to lose strategic partners or clients. This also can cause reputational damage or even might cause financial institution the risk of losing the license. will end up in fines. Audit recommendations, especially when it comes as major findings, and alerts high risk can be the significant motivator to start and prioritize anti-fraud software implementation in the company. In this case top management can be more involved and be more supportive.

When it comes to project managers, it is a very rare occurrence that they are aware with the technicalities of anti-fraud software, which makes this a highly unusual position. This might result in failed implementations, or a low level of priority being assigned. The top management or project sponsors should be responsible for the prioritizing of projects and the negotiation of resources required for the implementation project, which is a crucial responsibility.

According to the findings of the research, there is unquestionably a substantial correlation between the commitment and attention given by the company's leadership to the anti-fraud software implementation project and the project's success. The overwhelming majority of experts' comments indicated a direct relationship between success and characteristics relating to top-level commitment. In this case, it is necessary to incorporate the contextual aspect "Top management support" into the developed model. In addition, this variable should be treated as a critical aspect of anti-fraud software implementation projects because of its significance.

3.5. Fraud Team Commitment

Another contextual factor in the initial conceptual model derived from literature study was the qualifications and commitment of the fraud team during the project. This category was also emphasized in qualitative research. The experts were asked to evaluate the fraud team qualification and participation during the project implementation process.

The fact that not all the teams were working collaboratively meant that not all the experts were able to evaluate and respond to this question on the fraud team's commitment. Furthermore, experts who are members of the fraud team may submit responses that are deceptive or biased. Because of the previously indicated circumstances and limitations, only six experts' responses were considered in this variable assessment. Four of the replies indicate a strong relationship between project success and fraud team commitment. Expert 5, who indicated that the project was unsuccessful, also admitted that communication with the fraud team was problematic. The fact that they were located in separate countries might be the underlying cause of communication difficulties with the fraud team. The other 3 experts indicated their project as successful as well as positively evaluated fraud teams’ commitment. Telling, that fraud team “did a good job advising other teams and made sure everything is as in regulator's recommendations” (Expert 7) or simply evaluated their commitment as “excellent” (Expert 6).

Two experts, on the other hand, contradicted the connection between project success and the commitment of the fraud team. Expert 4 indicated that the project failed despite the fact that the fraud team had demonstrated a high level of commitment. Consequently, expert 2 regarded the project in which he was involved as a success, even though the fraud team's dedication had been less than adequate. Despite the fact that the fraud team had a lot of expertise, they were disinterested and did not want to be involved as much as they might have been.

To summarize the findings for this category, the engagement of the fraud team may be an important factor influencing project success. However, this study featured too many experts who were unable to evaluate fraud team commitment objectively. The half of experts’ responses had to be eliminated from this research question.

3.6. Software Suppliers Commitment

The following contextual factor from the initial conceptual model derived from literature study was the commitment from the software suppliers. The same way when analysing the commitment of the fraud team, three experts' responses should be also excluded from the software suppliers’ commitment category analysis. These three interviewees are from the software vendor or supplier side, and their responses might influence the misleading conclusions.

In one of the questions, experts were asked how they would evaluate the engagement, communication, and support of software vendors during the project's duration. Regardless of whether the project was successful or not, all experts rated software suppliers favourably. In the words of expert 3, “Software suppliers were always available, and you could always expect to get fast and quality feedback from them”. Other respondents place a high value on extensive supplier engagement, high-quality qualifications, and collaborative efforts. When asked about the attitude of the software suppliers during the contract negotiations and contract signing phase, expert 1 acknowledged that their team was satisfied with the results.

The outcomes of the commitment analysis of software vendors should not come as a complete surprise. They are in the business of providing a service, and their role is to be supportive and actively engaging in the project. Because of the lack of cooperation from service providers, their tool is unlikely to be picked in the first place. In contrast, it was anticipated that there may be certain unique scenarios in which the commitment of service providers could have an impact on the project's success. But according to the replies obtained, all experts were pleased with the communication, participation, and support provided by the service providers throughout the project.

To summarize, according to the findings of the research, the engagement of software suppliers is not a variable that can influence the success of a project. In addition, according to the findings of qualitative study, this contextual factor should be eliminated from the developed model.

3.7. Ethical leadership Impact on Anti-Fraud Software Implementation Project

The ethical leadership was the fourth contextual component of the conceptual model developed from the literature study that needed to be assessed in the practical part of the research. The experts received two questions regarding this research category – “How essential do you believe it is that the organization with whom you worked on the anti–fraud tool implementation project follows and supports an ethical leadership style?” and “Should such a company have a sense of social responsibility, and how can this be measured?”. By raising those questions there was a purpose to understand if the experts agree that ethical leadership and social responsibility are important factors for organisations. Another purpose was to clarify if there is a significant connection between ethical leadership and successful project of anti-fraud software implementation.

Detailed responses were provided, and all the experts, regardless of their position or level of experience, agreed that it is critical for organizations to adhere to an ethical leadership style and to have a sense of social responsibility. The expert 4 stated that for organisation it is very critical to follow the ethical leadership style in order to succeed at delivering transparent messages and clear communication. As well as regarding social responsibility, expert 6 declared that company should have the sense of social responsibility, and this should be measured through the strong alignment with different stakeholders and accurate tracking of variables like effort, cost, benefit, or value. Those responses fall under the subcategory of "transparent leadership position," which is considered to be a crucial component in the implementation of an anti-fraud programs.

The interviewee 5 highlighted important thought, stating that ethical leadership and social responsibility are important for the long-term success and partnership of the organization. Expert 1 shared the thought that “if company is trying to hide some fraud losses or are scared to see the real level of fraud they have – those projects will never succeed, there will be less attention for projects”. This response also reflects to the factor identified during literature review, which impacts struggles on fraud projects. For some leaders it could be beneficial to do not follow ethical leadership, or even fail with implementing anti-fraud programs, and this could be the reason why projects are receiving lower priorities.

Even, it was not straightforwardly asked, two experts shared, that the companies they were working on anti-fraud software implementation projects – "not always showed ethical leadership style" or "organisation had very low level of ethical leadership". Looking back at the project success review, both projects were generally considered unsuccessful. It is reasonable to presume that a lack of strong and clear ethical leadership among organizations might result in unsuccessful result of anti-fraud software implementation project. Furthermore, all experts support and agrees that it is essential for organisation, which is implementing anti-fraud projects, to follow the ethical leadership style and have a sense of social responsibility.

To summarize, ethical leadership is an important variable that has a substantial influence on the success of a project. Moreover, it is a critical component of assessing the specifics of anti-fraud software implementation projects.

3.8. The Challenges of Anti-Fraud Software Implementation Project

As an additional category of the questionnaire, experts were asked to describe the sorts of challenges they encountered while working on the anti-fraud software implementation project. This is also advantageous for gaining a thorough understanding of the complexities of such projects. According to the responses, the experts had highlighted a wide variety of distinct difficulties to address. There was no one spearheading challenge that stood out in comparison to others.

Expert 1 mentioned information technology resources and infrastructure shortages. The situation which expert encounters is that even the tool was with newest technological solutions, it was impossible to use the full functionality of the tool due to information technology infrastructure shortages within the company. Company was simply not collecting required datapoints. This challenge can be addressed as technological challenge from the client perspective or lack of maturity of organisation which is implementing anti-fraud solution. The "technological challenges" subcategory was followed by other respondents as well. Technical side of the project was also mentioned as challenging part of the project by expert 3. However, in this case the challenge was to adapt the technical side required to be in line with all law requirements and global practice.

The biggest challenge, according to the expert 2, was constantly changing legal requirements. The dynamics of anti-fraud technologies were also highlighted as a feature by few authors in the literature review. Expert 6 stressed another type of dynamics, stating that the most challenging difficulty for him was properly resolving unforeseen new variables encountered during implementation. This response also confirms another anti-fraud software specific identified during literature review – that software behaves very differently in different organisations This difference for Expert 6 appeared in new variables which were not considered in the project planning phase. Those responses fall under the subcategory of “dynamic software performance” which is considered to be a crucial characteristic in the implementation of an anti-fraud programs.

There were a number of experts who recognized challenges arising from legal responsibilities. Interviewee 7 emphasized that it was challenging to comply with legal requirements. The expert 2 underlined that, for the particular subject matter under consideration, legal requirements were continually changing, which had a significant impact and complicated the entire implementation process, according to him. Legal difficulties had an influence on the expert's 3 projects as well, as he underlined how challenging it was to obtain requirements from a wide variety of sources. The comments of those experts come under the "legal obligations" subcategory.

Another significant challenge, according to expert 2, was convincing other employees in the organization to use the fraud software and contribute to product development. This challenge was also underlined as the main challenge by expert 11. The challenge of encouraging other employees to participate to the project might be handled because of inadequate project scope communication or a lack of top management participation. Because if not all project stakeholders understand the significance of the tool and the importance of usage and engagement - it becomes significantly more difficult to get effective outcomes. This challenge falls within the "co-workers’ contribution" subcategory, and it will also be recognized as an important specific of anti-fraud software implementation projects.

Other experts highlighted the subcategory of “communication challenges”. One of the most difficult challenges during the anti-fraud software implementation project, according to expert 7, was communication with information technology teams. Expert 8 highlighted information sharing and communication across departments as a difficulty. Those comments indicate that, like any other project, anti-fraud software implementation projects are experiencing difficulties with efficient information sharing and task coordination among teams.

In his response, expert 10 indicated that the most difficult component of the anti-fraud software implementation project was defining the clear vision for how the product should perform and appear. This challenge can be also assigned to the subcategory of communication challenges. However, it demonstrates that there was no clear project scope defined at the beginning and that not all project team members were on the same page during implementation. This is one of the most critical challenges that might result in the failure of the project.

For a few experts, data interpretation and analysis proved to be a difficult aspect of the process. When asked about the primary challenge he encountered, Expert 9 stated that it was the correct data analysis and categorization of data that came from several distinct systems. It was also acknowledged by the interviewee 2 that their project team had difficulty locating the appropriate data in order to make data-driven decisions.

Another important factor that contributes to inadequate project management, according to the expert 5, is a shift in priorities. The expert noted that the change in priorities resulted in the project's failure. And it is a fact that no matter how good the project team or the software itself is, if top management does not prioritize the project, it will be impossible to assemble and obtain the resources necessary to complete the project successfully.

There were a number of additional challenges that were raised just by one of the experts and did not obtain any more support from the rest of the experts. Training, pricing, and the security of the organization are among those challenges.

In summarizing the category of challenges, the responses of the experts fell under seven subcategories of – “communication challenges”, “technological challenges”, “legal obligations”, "co-workers’ contribution", “data interpretation” and “dynamic software performance”. The following subcategories are given in the table 5. All the subcategories that were regarded to be critical characteristics in the execution of anti-fraud systems.

Table 5. Challenges identified during the project.

Category	***Subcategory***	***Interview statement***
Challenges identified during anti-fraud software implementation project	*Co-workers’ contribution*	*One of big challenges was to convince other employees to use the program and to help building the product.*
		People do not like changes, so it was hard to prove them, that the tool will be valuable.
	Technological challenges	*The most difficult thing was the technical side of the project*
		<…> technical implementation and technical decisions <…>
		<…> technical side needed to be brought into line with existing laws and global practice.
		IT infrastructure in my organisation. It is quite hard to build powerful anti-fraud engine when we are not simply collecting many datapoints from our clients. We simply cannot use full functionality of the tool.
	Communication challenges	*Information and communication between departments <…>*
		Usually, the natural language understanding part was challenging <…>

		<…> there was miscommunication <…>
		Hardest part is to clarify the vision how tool should work and look <…>
	Legal obligations	*<…> in line with existing laws and global practice.*
		<…> hard to collect legal requirements from different sources <…>
		Most significant- complying with the regulations <…>
		<…> constantly changing legal requirements for particular question, e.g., every 3-6 months.
	Dynamic software performance	*<…> addressing of unexpected new variables.*
		<…> new cases appear as time goes on.
		<…> The proper addressing of unexpected new variables faced during the implementation
	Data interpretation	*<…> find the right data in order to make data driven decisions.*
		Mainly data analysis, to differentiate data coming from different systems and their categorization.

Source: Composed by the author

3.9. The Root Causes of the Project Failures

Following the identification of the most significant challenges associated with the implementation of anti-fraud software, the category of root causes of project failures was established. Experts were requested to share their perspectives on what they believed to be the core causes of anti-fraud software implementation project failures or postponements.

The most frequent response was related to leadership role in the project and falls under the subcategory of "top management commitment ". Experts were mentioning low priority for the project, lack of involvement or attention from the top-management, shift in priorities or not enough resources delegated. These comments in response lead to previously analysed component from the conceptual model– top management commitment. And once again demonstrates how this contextual aspect influences the effectiveness of anti-fraud software implementation projects. Experts also noted inaccurate scope definition, over-ambitiousness that led to disappointments, and replacing project managers in the middle of the project as root causes leading to the project failures. These issues might also be avoided with adequate senior management commitment.

Another prevalent explanation cited by experts was a shortage of qualified human resources or an inefficient distribution of available human resources. This was the condition that was mentioned by a total of five participants. The lack of resources may be attributed to inadequate project management, improper planning, and, once again, a lack of attention from the company's leadership. The “shortage of resources”, on the other hand, should be classified as a separate subcategory, as it has been explicitly addressed by a significant number of experts.

The subcategory of “lack of basic knowledge of project management” was also popular among experts’ answers. Expert 1 highlighted that one of the main causes which might lead project to failure is no proper ownership of the project. There simply was not clear who should lead the project and take the ownership of tasks. Expert 6 added that failures of the project are caused by wrong definition of the scope and wrongly estimated project costs. Interviewee 12 mentioned unclear project planning and changing project manager without proper distribution of the tasks among the teams. All those responses represent the limited knowledge of basic principles of project management.

The other cause which might affect project postpones or failures was categorized as subcategory of “wrong tool selection”. Few experts were indicating this aspect. It was already identified in theoretical research, that tools might completely differently behave in different environments, and therefore additional in-house testing phase is required prior to software implementation to reduce the risk of underperformance. Unfortunately, not all organizations choose in-house testing, which exposes the organization to the risk of picking the incorrect solution.

A few experts mentioned excessive tool complexity as a likely reason for project failures and postponements. Expert 9 emphasized the data management and complicated architecture of the software. This falls under the subcategory of "complexity", which is considered to be a crucial characteristic in the implementation of anti-fraud projects. During the literature review, the complexity of anti-fraud solutions was also recognized as a technological characteristic and a high likelihood of challenge. Because fraud detection software must be constructed using constantly changing and adaptable algorithms, technical solutions are difficult to implement. Furthermore, to create the most accurate fraud scores and detect fraud, organizations need to provide a wide range of different datapoints to the service provider. Those datapoints are not always straightforward to gather and deliver. If it was not discovered during the project planning phase, it poses additional impediments that may result in project delays. And, based on the qualitative research, it appears that the project management approach was not always followed correctly inside the experts’ organizations.

From the other side – expert 4 notices an important aspect related to complexity avoidance. When an organization faces complexity issues and decides to avoid the complexity and minimise the scope by choosing only a few fraud patterns that they are willing to catch or using strict prevention methods, this might also cause the anti-fraud project to fail. According to the expert, it ends up in poor operation of the tool and limits the possibility of identifying the most recent fraud patterns. However, organizations may determine the scope based on their requirements, and if their initial intention was to limit the fraud patterns to a minimum, that might be perfectly acceptable. The problem develops when an organization repeatedly changes the scope of the project due to its complexity and simply chooses a lower-quality product as a result.

Expert 11 mentioned legal difficulties as potential reasons for anti-fraud software implementation project delays. Legal considerations may exacerbate the difficulties and increase the time required to accomplish the task. The expert specified internal policies alignment with the software suppliers' legal procedures. This is a complicated problem since both parties are signing agreements that must be favourable to their respective sides. It may be difficult to create a consensus if the agreement is not based on global legal standards and has one-way methods.

The last group of factors identified by the experts falls under the subcategory "issues with the data" and is described below. Two respondents said that they have recognized data difficulties, such as data tardiness and inadequate data management, as a possible explanation for project failures and postponements involving anti-fraud software implementation projects.

Table 6 presents a summary of the findings from the category of root causes of project failures. Seven subcategories were identified and provided in the table together with supporting statements made by the experts. Those subcategories are "top management commitment ", "shortage of resources", "wrong tool selection", "complexity", "issues with the data", "lack of basic knowledge of project management", and "legal difficulties".

Table 6. The root causes of anti-fraud software implementation failures and postpones

Category	***Subcategory***	***Interview statement***
The root causes of anti-fraud software implementation project failures and postpones	*Shortage of resources*	*<…> Lack of qualified testers <…>*
		Lack of resources <…>
		Not enough support from experienced colleagues <…>
		<…> resource allocation as in employees and hardware etc
	Top management commitment	*<…>low priority for the project <…>*
		<…>and lack of involvement of management.
		<…> low attention from top management, <…>
		<…>lack of support from organization.
	Wrong tool selection	*<…>the tool which was selected is simply not working for the company – do not provide expected results.*
		Tool not being perfectly suitable for a certain organization.
	Legal difficulties	*Legal issues, internal policy alignment with the new tool <…>*

	Complexity	*<…> complicated architecture.*
		The complexity of the system, which correlates with development time <…>
	Issues with the data	*There were errors in data and data delays <…>*
		Data management lead to failure <…>
	Lack of basic knowledge of project management	*<…> As well there were no ownership of the project <…>*
		Wrong definition of the scope and the estimated costs.
		<…> unclear planning <…> changing project managers, and team without distribution of tasks.

Source: Composed by the author

3.10. Anti-Fraud Software Implementation Projects' Lessons Learned

The following categories analysed during qualitative research were related to professional opinion of the experts, regards anti-fraud software implementation projects. The experts were asked to discuss the most important takeaways or lessons learnt from the anti-fraud software implementation projects. Experts gave detailed responses to this subject, sharing their experiences and lessons learned.

Expert 1, who was taking on the role of fraud manager in the software implementation project, explained that he learned not to expect stakeholders to take full responsibility and execute their jobs well. If you really want to acquire a decent quality product, you should keep yourself involved as much as possible as the primary user of the tool. An expert also advises being prepared, as the outcome may not be as pleasing as expected during the software suppliers' demonstrations. The same subcategory of “unsatisfactory outcome” was noted as a takeaway by expert 11. He stated that the process typically takes longer than planned and that the results are not always what they were expected. Typically, if the results are unsatisfactory, software suppliers will express it, based on a lack of your organization's setup or poor data quality.

Expert 4, who participated as a fraud prevention analyst during the project, similarly identified full engagement and ongoing monitoring of implementation progress as a significant takeaway. He also emphasizes reporting methods, corrective actions, and quality assurance as elements that should be included in similar projects in the future. Experts 1 and 4 answers indicated that the key users of the anti-fraud software are taking lessons, that project implementation requires constant monitoring from their end. Otherwise, the implementation is not progressing as planned. Expert 5 shared a similar takeaway, emphasizing the need of establishing an evaluation system to track performance of the team as soon as possible. Those responses fell into subcategories of “full engagement during the project” and “tracking project performance”.

According to experts 3 and 8, the most important lesson they learned while working on anti-fraud software implementation projects was the need of being patient. As specialists and software testers, respectively, they were each assigned to various responsibilities over the project's duration. Further to that, when it comes to project execution, hard labour may genuinely move mountains, according to the expert 3. Those responses fall under subcategory of “patience and hard work”.

It is essential, corresponding to the expert 2, to have everyone on the same page. Whole organization should grasp the tool's additional value and trust it. Feedback from organization employees, users, or developers is a highly valuable component for future developments and improvements. That is why it is important to have teams that are willing to provide comments and suggestions. Expert 6 completely agrees with this objective, emphasizing adequate engagement of all essential stakeholders. Additionally respondent complements, that an agile project management approach should be used for anti-fraud software implementation projects. “Organizational participation” and “feedback on software performance” are the subcategories composed of the comments from these two experts.

Keeping with the same theme of team’s involvement – the importance of teamwork and ability to use team’s potential are lessons learnt from couple of other experts. Expert 7 stated that collaboration is what makes the work happen. The expert 10 agrees on importance to have assigned team to handle the project and emphasizes that different experiences from team members and their suggestions might help to avoid risks and failures.

Expert 9 emphasizes the necessity of planning and data management as critical takeaways from the anti-fraud software implementation project. Expert 12 also gained similar experience and took similar take away. He goes on to explain that there is always a need to plan and communicate what you are preparing. Also, those projects are difficult to manage, and if you are working on them or plan to work on them, you should fight for the resources required. It this is impossible unable to obtain the necessary resources, there is no point in starting the project. Those responses fall under the subcategories of “project planning” and “data management”.

Other takeaways or lessons learned which were mentioned by expert 5 were management of complexity and maintaining the rate of delivery over the duration of the project. The subcategory of complexity of anti-fraud software projects was identified early in the literature research and qualitative analysis. As a result, even highly experienced software engineers may find it difficult to handle the specifically high complexity level. Due to the project's complexity, achieving and keeping a high delivery rate becomes more difficult.

The final subcategory which was distinguished from the responses of the experts regards lessons learnt was entitled “team and human resources”. Expert 10 underlines the need of assigning a team to work on anti-fraud projects in order to accomplish them successfully. In addition, he said that the team brings diversity and variety of different experiences from team members and their recommendations may be useful throughout the project's execution. Expert 12 continues to emphasize the necessity of working as a team throughout the project's execution and acknowledges that the project manager should fight to ensure that the necessary human resources are given to the project. Attempting to complete the job in any other manner would be difficult.

To summarize the lessons gained and important takeaways from the anti-fraud software implementation projects, experts emphasize the necessity of large number of details to be considered. Those details of responses fall under the subcategories of “project planning”, “data management”, “complexity”, “organizational participation”, “feedback on software performance”, “full engagement during the project”, “tracking project performance”, “unsatisfactory outcome”, “patience and hard work” and “team and human resources”. Table 7 represents all the subcategories as well as statements from experts' answers and opinions.

Table 7. Anti-fraud software implementation projects' lessons learned

Category	***Subcategory***	***Interview statement***
Anti-fraud software implementation projects' lessons learned	*Project planning*	*<...> that project is hard to handle, that you need to plan and communicate constantly <...>*
		<...> planning <...> is very important <...>
	Data management	*<...> data management is very important<...>*
	Complexity	*Manage the complexity and keep the rate of delivery <...>*
	Organizational participation	*The most important part is to get everybody onboard: that all organization would want to use the tool <...>*
		Proper inclusion of all relevant stakeholders <...>
	Feedback on software performance	*<...> all the organization would trust that system and would be willing to provide feedback for further developments.*
		<...> Different experience and suggestions might help to avoid more risks of failure.
	Full engagement during the project	*Do not expect that people will do their best. You have to be involved in every part of the project <...>*
		<...> On-going monitoring.

		<…> you need to plan and communicate constantly.
	Tracking project performance	*Reporting procedures, Corrective action, Quality assurance <…>*
		<…> keep the rate of delivery, set-up an evaluation framework early on.
	Unsatisfactory outcome	*<…> the results might be not so successful as you expected <…>*
		It takes time and thing do not always go as planned.
	Patience and hard work	*Most important lesson I've learned was that patience and hard work could move the mountains*
		I have learned patience
	Team and human resources	*Teamwork makes the dream work <…>*
		It should be a team that would work on such projects.
		<…> you should fight for resources, or if there are no proper human resources - then do not initiate the project.

Source: Composed by the author

3.11. Experts' Advice for the Project Managers

The last question asked for the interviewed experts was asking what advice interviewee can provide to the project managers who are working or will be working on anti-fraud software implementation projects in the future.

The most frequent advice addressed the "senior management's position" subcategory. The expert 1 recommended paying particular attention to the project prioritization level. Expert 12 agreed with this approach and emphasized the importance of understanding the project's leadership position. Top management should support the anti-fraud culture and have a low or zero tolerance for fraud. If the project is not on the company's priority list, the project manager should either fight for the priority or get rid of the project. Low prioritizing will lead projects to problems with resources, postponed due dates, low budgets, stakeholder commitment, and so forth. Expert 2 provides the same advice as expert 1, which is to try to acquire approval from upper management and other managers.

Other experts expressed concern and suggested that communication should be prioritized. Expert 10 advises that you should not be embarrassed to seek assistance from other team members. It might be difficult to ask for help in certain instances, but in the majority of cases, particularly when you are struggling, it can be quite beneficial to seek advice from co-workers who have previous experience with the issue. Or, at the barest minimum, they are capable of problem solving. You should always encourage your colleagues and make follow-up calls or emails to ensure that everyone is on the same page throughout the implementation process, according to the expert 10. Those responses fall under the subcategory of “effective communication”.

The expert 9 advice project managers to clarify small details, starting with what data is needed for the tool and what needs to be done with that data. In order to combat fraud, the anti-fraud software depends on data and delivers data back. Even if the project manager does not have a very strong technical background, understanding the details is an essential aspect. Interviewee 1 also provides the recommendation to pay attention to the details and try to understand them. Attention to details was also the main advice coming from the expert 5. Those responses belong under the subcategory of “high attention to the details”.

Expert 6 recommends anti-fraud software implementation project managers to begin with a very clear definition of the project's scope and expected outcomes. Additionally, it is important to get all stakeholders on the same page and get their opinion on the project's expected outcomes. Those recommendations fall under the subcategory of “clearly defined project scope”. An agile project management methodology, according to Expert 8, should be used in such implementation activities. Considering the previously indicated dynamism and complexity, an agile project management technique may prove to be a practical solution.

A strict approach may not be advantageous in anti-fraud software implementation projects, according to the interviewed expert 3. He advised project managers to be patient and open-minded to other points of view. Expert 7, who participated as an anti-money laundering expert on the project, recommended including as many tools as possible in the first evaluation. Having a larger pool of potential tools increases the likelihood of selecting the most suitable one. Therefore, conducting thorough market research from the start might save you a lot of time in the long run. Responses from expert 3 and expert 7 fall under the subcategory of “open-mindedness”. Expert 4 emphasizes the importance of preventing fraud in the first place rather than detecting it after the fact of fraud. The expert also shares his experience, stating that in practice, the same processes and controls established in place to prevent fraud may also be used to detect fraud.

Summarizing experts' advice to project managers now working on or planning to work on anti-fraud software implementation projects, the essential category of advice is to understand and pay close attention to details. Among these details is senior management's position on the tool and the tolerance level for fraud in organizations. Additionally, details may be related to the technical aspect of the project. Furthermore, experts advocated sticking to project management essentials such as defining the scope of the project clearly, involving all important stakeholders, and maintaining effective communication throughout the project. All those details fall under different subcategories of “senior management's position”, “leadership’s tolerance level for fraud”, “high attention to the details”, “clearly defined project scope”, “effective communication” and “open-mindedness”. Table 8 contains a list of the subcategories as well as the remarks extracted from the experts’ statements.

Table 8. Experts' advice for project managers working on anti-fraud projects

Category	***Subcategory***	***Interview statement***
Experts' advice for project managers working on anti-fraud projects	*Senior management's position*	*<…> try to get green light from top management and all other managers.*
		If project is not prioritized – leave it or fight for priority. There will be no resources and you will end up with trouble.
		Understand the leadership role position in the project. <…>
	High attention to the details	*Start super small, nanoscale, then grow your ambition.*
		Try to understand every detail <…>
	Clearly defined project scope	*Start with a very clear definition of the scope and expected outcomes collected from all relevant stakeholders.*
		Be clear on what data you need and what needs to be done with it.
	Effective communication	*<…> Keep good communication <…>*
		Ask for more advice, support, and follow ups from colleagues and organization.
		Communication to give information and receive feedback.
	Leadership’s tolerance level for fraud	*<…> if they do not support fraud culture- do not start the project. It will be hard <…>*
	Open-mindedness	*Be patient, be curious and be open minded to various opinions*
		Pick as many as possible tools for initial review.

Source: Composed by the author

3.12. Discussion and Results from Qualitative Research

The primary objective of qualitative research was to validate the contextual components identified in the initial conceptual model developed from the literature review. Following comprehensive qualitative research, the contextual factors in the developed model can be modified and replaced. The responses of the experts demonstrated unambiguously that the involvement of a software provider component has no substantial influence on the success of an anti-fraud software project. A unanimous consensus was reached by all the experts regarding the evaluation of suppliers' cooperation and participation. In addition, it has been concluded that this has no impact on the overall performance of the project. Consequently, according to the findings of the qualitative investigation, this contextual factor should be eliminated from the developed anti-fraud software success model.

A significant correlation has been discovered between the performance of anti-fraud software projects and contextual factors such as senior-level management commitment, ethical leadership, and the qualifications and involvement of fraud teams, according to qualitative study findings. It was determined that those three elements were acceptable, and they would be included into the model that has been developed.

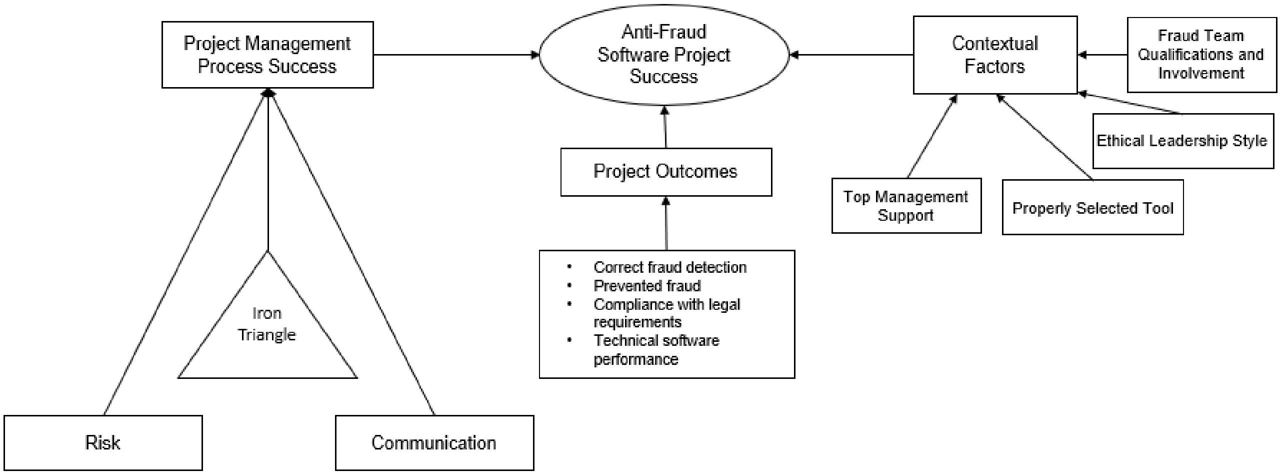
Project Management Process Success
Anti-Fraud Software Project Success
Contextual Factors
Fraud Team Qualifications and Involvement
Ethical Leadership Style
Project Outcomes
Top Management Support
Properly Selected Tool
Correct fraud detection
Prevented fraud
Compliance with legal requirements
Technical software performance
Iron Triangle
Risk
Communication

Figure 7. Developed Anti-Fraud Software Implementation Project Success Model. Composed by the author.

Additionally, several parameters were incorporated into the developed model because of extensive qualitative research. It has been demonstrated that the appropriately selected tool contributes considerable value and has a significant impact on the success of the anti-fraud software implementation project. The software itself could have a considerable influence on the component that deals with project results. The project execution phase might be successful, but poor software quality could lead to unsatisfactory project results. Moreover, it was clarified that the process of choosing the tool is outside the scope of the project and should be completed prior to the project's commencement. The appropriate tool selection, as well as in-house testing of the software, may have a significant influence on the results and how the tool performs once it has been implemented. Furthermore, it could overcome risks and challenges created by complexity and dynamics, data difficulties or technical software performance, as well as unsatisfactory results. This component cannot be considered as traditional project management success factor or project outcome. There is significant value in this component, and it has been shown to be a more valuable attribute than the "commitment of software suppliers". Therefore, the component "software suppliers' commitment" will be replaced by the component "properly selected tool" in the contextual factors section of the model that has been constructed (figure 7).

The primary objective of the qualitative study was to analyze the contextual elements that influenced the initial conceptual model; nevertheless, the project outcomes were taken into consideration as part of the overall research. The project outcomes part of the initial model includes components such as "correct fraud detection," "prevented fraud," and "business continuity". “Correct fraud detection” and “prevented fraud” were frequently highlighted as essential components by the experts in a variety of topics, including the anti-fraud software project success criteria category. Therefore, those two elements were determined to be valid and will be incorporated into the model that has been developed. However, “business continuity” did not appear to be an important parameter for the experts, and therefore, this component was excluded from the developed model.

Some of the components represent anti-fraud software characteristics that must be considered as project outcomes that demonstrate the successfulness of the anti-fraud software implementation project. Experts highlighted "compliance with legal requirements" as one of the most important elements to consider. This parameter was recognized as a critical component in determining whether the project was successful. In fact, this parameter is one of the most significant discoveries from qualitative research since it was not considered during the theoretical research. According to the experts who participated in the research, "technical software performance" is an additional parameter that should be considered a success factor. Some of the characteristics highlighted in relation to this component are the ability to automate the process, the avoidance of false positives, and the incorporation of recognized fraud scenarios. As a result, the subcategories "compliance with legal requirements" and "technical software performance" were identified as significant project outcomes components and were included in the model that was built as project outcomes.

Market research, in-house software testing, and a combination of market research and in-house software testing are three subcategories that experts have identified and underlined in relation to the selection of fraud-prevention software. Experts also stated that they were involved in the implementation project, which did not necessitate the selection of a tool because it had been completed in a previous stage. As a result, based on their previous expertise, project selection and implementation were handled as separate projects.

The secondary objective of the qualitative research was to determine the requirements and main characteristics of anti-fraud software implementation projects. In the interview, the experts' perspectives on specifics of anti-fraud projects were identified based on their previous experience working on anti-fraud projects. The experts brought to light other components that they consider would benefit the success of a project to implement anti-fraud software or at least should be considered as possible triggers for challenges or failures. Summarizing experts statements regarding questions, which required to share their personal opinion regards lessons learnt, project uniqueness, encountered challenges, projects' success factors, root causes for failures and advices for the other project managers it appeared, that the most popular highlights were related to the traditional project success characteristics (20%), the need to be compliant with legal requirements (12%), complexity and dynamics of the software (11%), technical software performance (8%) senior management's commitment (8%) or organizational participation and contribution (8%). Figure 8 represents a pie chart illustrating the distribution of groups of subcategories identified during qualitative research.

According to the experts, most of the components mentioned as being important to consider during anti-fraud software implementation projects reflect the traditional project success characteristics. Those characteristics include project planning, effective communication, clearly defined the project scope, completing project within time and on budget, tracking project performance and quality, involvement of all relevant stakeholders. The part of experts is considering those factors to be highly important in anti-fraud software implementation project. This indicates that an anti-fraud-related project should be managed in accordance with standard project management standards and high attention to effective communication or clearly defined scope to all of stakeholders. However, there are other variables that must be addressed, and which are not included in classic project success frameworks, such as the Iron Triangle.

The group of subcategories relating to compliance with legal requirements is the second most common collection of subcategories that has been identified. This group was mostly highlighted mentioning the project uniqueness and encountered challenges. Because this characteristic of anti-fraud software projects was not recognized in the literature research, it may be considered a significant finding from the qualitative research. Complying with legal, regulators or audit requirements, could be the significant driver for implementing anti-fraud software in the organization. In addition, having adequate fraud detection techniques has become a required element for a large portion of organizations to be successful. Organizations that operate in the financial industry, in particular. If this is not the case, the organization may be penalized by local authorities.

Complexity and dynamics fall under the third most popular group of characteristics, which were discovered throughout the comprehensive qualitative research. The complexity of the software and its architecture, as well as unanticipated performance or dynamics that were discovered during the implementation, were all noted by the experts in the discussion. When discussing the uniqueness of anti-fraud software implementation projects, experts tended to emphasize the characteristics listed above the most often.

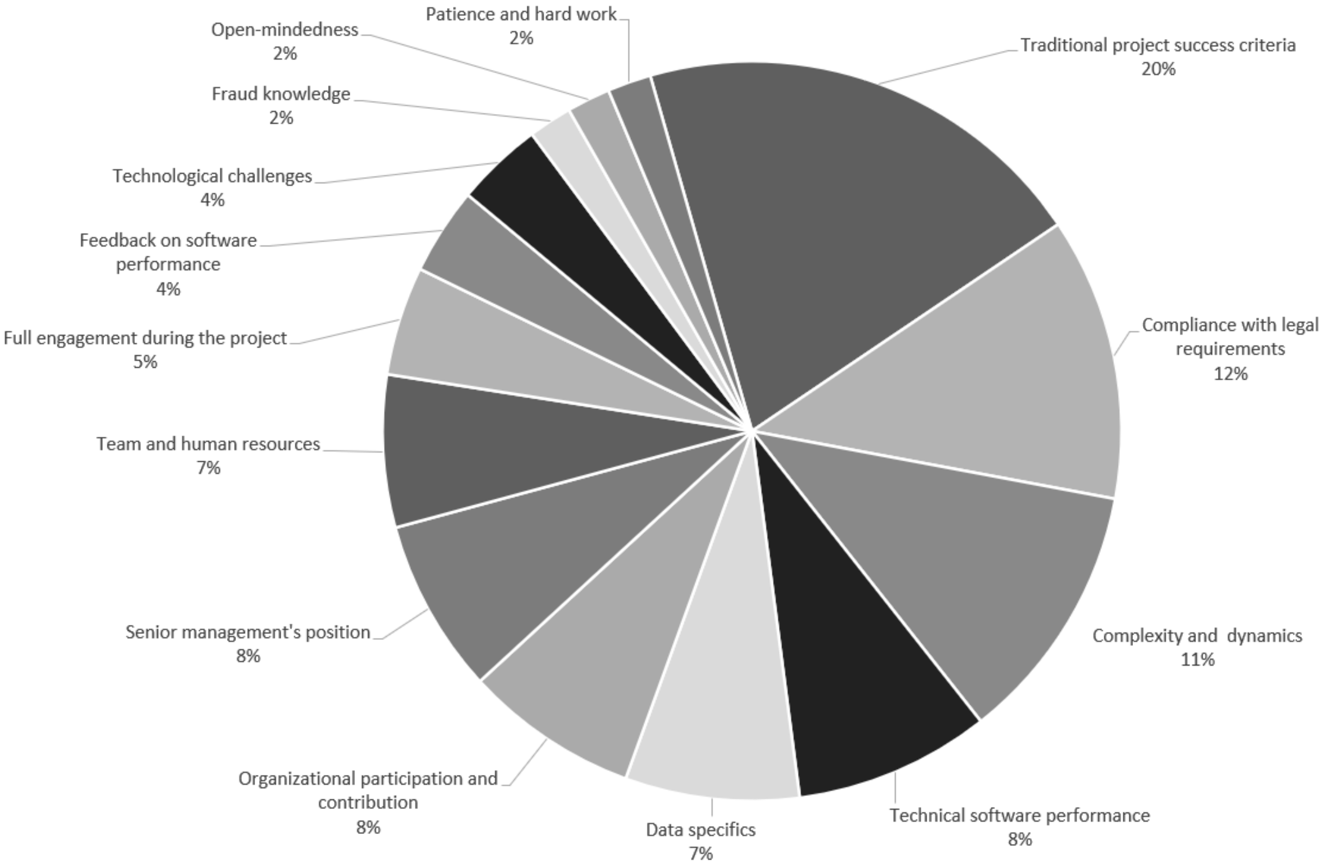

Figure 8. The Distribution Among Groups of Subcategories Identified During Qualitative Research. Composed by the author.

The examination of expert responses to the interview categories additionally resulted in the formation of several additional groups of subcategories that demonstrated the significant characteristics of anti-fraud software implementation projects. These additional groups correspond to characteristics such as technical software performance, data specificity, team and human resource engagement, senior management participation, and organizational participation and contribution. Those subcategories were repeated across several categories, which provided stronger justification for their inclusion as a feature of the characteristics of the anti-fraud software project.

In addition, groups that were mentioned less often but were strongly reasoned by experts were the need for the project manager to be completely engaged in the project and pay attention to details, analyzing feedback about software performance, or general fraud knowledge.

4. CONCLUSIONS AND RECOMMENDATIONS

4.1. Theoretical Research Conclusion

The theoretical research resulted in the identification of several categories of specifics which include management approach related specifics like position of the leadership regards fraud relevance, the necessity of proactive and forward-thinking strategy or importance of ethical leadership. Additional specifics were appropriate fraud resource delegation and competencies of the team which will be handing fraud fighting. Other set of considerations includes technical peculiarities of anti-fraud software, including complexity, dynamism, vast quantity of requirements, and fact, that the program performance relies on many different aspects and could operate entirely different for various organizations. Although, it is necessary to comprehend the fundamentals of project management in order to successfully execute an anti-fraud software implementation project. Theoretical research also came to the conclusion that the classical and fundamental successful project management criteria such as completing projects on time, within budget, and with high quality are essential. Other findings included taking into consideration potential risks and placing a strong priority on effective communication.

The conclusions of the theoretical investigation resulted in the establishment of a conceptual model for the success of anti-fraud software implementation projects. The model was developed by incorporating several project success models previously proposed by other researchers, as well as new factors that were discovered via theoretical research and have been shown to be relevant to anti-fraud software projects. The conceptual model for anti-fraud software implementation success contained three constructs: the success of the project management process, the outcomes of the project, and the contextual factors. The traditional project success criteria, which were a significant topic of discussion among academics, were represented by the success of the project management. The project deliverables were represented by project outcomes. The characteristics that were identified as specifics of anti-fraud software projects during theoretical research were referred to as contextual factors in the conceptual model. Those characteristics were top management support, involvement of software providers, ethical leadership, fraud team qualifications and involvement.

4.2. Contextual Factors Impact for Project Success

The contextual factors as well as their implications for project success, were emphasized during the empirical research phase. According to qualitative research results, a substantial link has been observed between the successful anti-fraud software projects deployment and contextual elements such as senior-level management commitment, ethical leadership, and the qualifications and engagement of fraud teams. This demonstrates that leadership engagement and leadership ethics have significant effect on successful anti-fraud software implementation. Moreover, it is vital for company to allocate experienced fraud professionals who should be completely engaged throughout the process.

According to the findings of the experts who were interviewed, the engagement of software suppliers does not have a substantial influence on the success of anti-fraud projects. Consequently, this factor was eliminated from the developed model for anti-fraud software implementation project success. Another contextual component – appropriately chosen anti-fraud software – filled the void left by the previous one. The software itself may have a significant impact on the component dealing with project results. Although the project execution phase may be effective, inadequate software quality may result in unsatisfactory project results.

4.3. Project Management Process Factors

The fundamental project management process success factors were identified to having significant impact for anti-fraud software implementation project. As any other project anti-fraud project should follow the traditional project management principles as effective communication, completing project within budget, time and high quality or proper risk management. Additionally, experts highlighted establishing a clearly defined and communicated scope of the project, scheduling, and budgeting for the project's workflow, identifying risks, and achieving project goals and objectives that were initially established but subsequently acknowledged. All those elements have been categorized under project management process construct and have significant impact on anti-fraud projects success.

4.4. Project Outcomes

Additional construct included in the initial conceptual model was project outcomes. When it was first developed, it featured accurate fraudulent detection and fraud prevention, as well as business continuity. Correct fraud detection and prevention proved to be essential project outcomes that contributed to the project's overall success. However, after a comprehensive empirical investigation, it was shown that business continuity is not a criterion that is particularly relevant for anti-fraud initiatives.

The compliance with legal requirements and the technical performance of the software proved to be a more significant factors to take into consideration and were incorporated into developed model. Legal restrictions, according to a large number of experts, are the primary driver and challenge for the deployment of anti-fraud software. In the end, software should be compliant with all applicable legal requirements. As a result, this component was selected as a considerable project outcome that reflects the overall success of the project. An additional project result was the technical software performance, which suggests that if the software is adaptable, convenient to use, and the feedback about the tool is favorable, it contributes to evaluating if the project was successful.

4.5. Specifications of Anti-Fraud Software Projects

The examination of expert responses to the interview categories additionally resulted in the formation of several subcategories that demonstrated the characteristics and specifications of anti-fraud software implementation projects. There were many of those subcategories that were repeated across several categories, which provided stronger justification for their inclusion as a feature of the characteristics of the anti-fraud software project which should be considering during those projects. The leading subcategories were already mentioned and incorporated into developed project success model – traditional project success criteria, compliance with legal requirements, technical software performance and senior's management position or contribution. Furthermore, additional project characteristics were identified – complexity, dynamics, importance of data specifics, organizational participation and contribution, requirement for full engagement.

4.6. Selection of Anti-Fraud Software

The importance of properly selected anti-fraud software was indicated as being significantly important factor for successful project completion. The comprehensive empirical research, proved, that selection of the tool is usually done as a separate project and is out of the anti-fraud software implementation project scope. The experts' recommendations are to perform a deep market research and in-house software testing. However, it also showed up that clearly defined requirement and expectations can have an influence in proper tool selection.

4.7. Recommendations and Principles for Anti-Fraud Software Implementation Projects

In addition, qualitative research was conducted in order to provide practical implications by determining the principles and requirements of projects for the implementation of fraud-fighting technological solutions. Twelve experts who have been involved in anti-fraud software implementation projects were interviewed with the purpose of obtaining practical implications for the research. The experts were representing different organizations and were having different responsibilities and roles during the projects. Therefore, their responses and summary of their responses led to comprehensive understanding of anti-fraud projects. Consider the issue from several perspectives rather than focusing exclusively on one.

The following are the recommendations for future project managers or other stakeholders of the anti-fraud software implementation project, based on a summary of theoretical and practical research findings:

1. The use of traditional project management principles to the implementation of anti-fraud software is recommended by this research, which is the first and most essential recommendation made by this study. The fundamental project management elements include establishing a clearly defined and communicated scope of the project, scheduling, and budgeting for the project's workflow, identifying risks, and achieving project goals and objectives that were initially established but subsequently acknowledged. Due to the fact that anti-fraud initiatives are currently confronted with this difficulty in reality, the ownership of the project is also an extremely important factor to take into consideration. The ability to communicate effectively is crucial, especially when it comes to establishing the project scope and goals, bringing all stakeholders together, and providing and receiving feedback throughout the lifecycle of the project.
2. The other recommendation from this research is to make it absolutely clear what the leadership's perspective on fraud is and how much tolerance the organization has for fraud. Even though it was one of the most significant components identified during the literature review phase, the experts' perspectives were also affirmed throughout the qualitative research phase. The role of senior management in the prevention and detection of fraud is fundamental. Furthermore, without their cooperation, it will be substantially more difficult to move forward with the project. It is also essential that the company adheres to an ethical leadership style, which means that the organization promotes respect and service to others, develops community, and demonstrates honesty and fairness.
3. The following guideline is to pay close attention to the details and to be completely involved in the project throughout its duration. According to the findings, anti-fraud projects have also been discovered to be exceptionally complex and dynamic. A high degree of concentration and consistent attention to detail are necessary to operate with anti-fraud technologies in an efficient and effective way.

4. Another recommendation that was brought to light during the practical investigation is the need to comply with legal requirements. It is becoming more important for legal and audit recommendations to be followed, especially in the financial industry. As a consequence, anti-fraud programs are also being affected as a result of these developments. First and importantly, it may act as a great accelerator and motivator for the implementation process, both in terms of speed and intensity. However, it can also result in more stringent requirements or overall complexing of the project by including additional stakeholders or clearly specifying the outcome.
5. One of the most significant outcomes of this type of project is the improvement in technical software performance or the ability to detect and prevent fraud. Consequently, it is critical to collect feedback from the primary users while also testing the program and attempting to gather experts in order to reach the best possible outcome. Unsatisfaction with the outcomes of the instrument was a trait that was frequently stated by the experts during the interview and was identified as such.
6. Additionally, this research has found that the selection of the appropriate tools is a critical responsibility during the implementation of anti-fraud software. Even though this is often beyond the scope of a project, it has a significant influence on the overall success of the project. In spite of the fact that it was not included in the original scope of the project, the project manager is typically responsible with putting the tool into operation. During the project scoping phase, the project manager can bring up this subject for discussion. There should be stakeholders who accept responsibility and ensure that the tool has been thoroughly tested and that its features have been thoroughly reviewed before it is chosen for use. If this would not be done, even the most well-managed project can wind up with poor outcomes — a tool that is just not effective for the organization and is not detecting and preventing frauds.
7. For the effective application of an anti-fraud technology, it is also necessary to have appropriate competencies and attitudes. Data analytics and fraud intelligence are two of the competencies that are in high demand these days, respectively. Some of the attitudes that have been highlighted include open-mindedness, patience, and a willingness to put in the necessary effort.

4.8. Limitations and Suggestions for Future Research

The examination of expert responses to the interview categories additionally resulted in the identification of several limitations of the research. The first constraint that was identified was the vast extent of the experts. On the one hand, it provided a more comprehensive view from a variety of perspectives. However, for certain of the research categories, it was necessary to exclude some experts in order to avoid biasing the results. Future research would benefit from analyzing and looking deeper into particular roles within the project in order to gain a better understanding of the significance of those responsibilities.

Likewise, another approach that might be used to gain a deeper understanding of this topic is to look at unsuccessful projects as a case study and analyze those from different perspectives. This means that multiple departments such as project management, fraud team, leadership, or technical support should be involved in conducting interviews with experts in this area.

LIST OF REFERENCES

Abdullahi, R., 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 Vol. 5, No.4 38-45. https://dx.doi.org/10.6007/IJARAFMS/v5-i3/1823

Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021*). A Semantic Rule Based Digital Fraud Detection*. PeerJ. Computer Science, 7, https://doi.org/10.7717/peerj-cs.649

Al-Hashedi, K. G., & Magalingam, P. (2021). *Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019.* Computer Science Review 40.

Amasiatu, C. V., & Shah, M. H. (2018). *First Party Fraud Management: Framework for The Retail Industry*. International Journal of Retail & Distribution Management.

Ann Riney, F. (2018). *Two-Step Fraud Defense System: Prevention and Detection.* The Journal of Corporate Accounting & Finance, 29(2), 74–86. https://doi.org/10.1002/jcaf.22336

Association of Certified Fraud Examiners. (2020). *Report to The Nations. 2020 Global Study on Occupational Fraud and Abuse.* https://www.acfe.com/report-to-the-nations/2020/

Baader, G., & Krcmar, H. (2018). *Reducing False Positives in Fraud Detection: Combining the Red Flag Approach with Process Mining*. International Journal of Accounting Information Systems, 31, 1-16.

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Bartsiotas, G. A., Achamkulangare, G., (2016). *Fraud Prevention, Detection and Response in United Nations System Organizations*

Beneish, M. D., Vorst, P., (2021). *The Cost of Fraud Prediction Errors.* Kelley School of Business Research Paper No. 2020-55, Available at http://dx.doi.org/10.2139/ssrn.3529662

Bobinas, I. (2018). *Sukčiavimo Aptikimas Bekontakčiuose Elektroniniuose Mokėjimuose: Magistro Darbas*. Vilnius University. 22-23.

Bolton, R. J., Hand, D. J. (2002). *Statistical Fraud Detection: A Review. Statistical Science*. 17(3), 235–249. https://doi.org/10.1214/ss/1042727940

Brown, M.E.; Treviño, L.K.; Harrison, D.A. (2005). *Ethical leadership: A social learning perspective for construct development and testing.* Organizational Behavior and Human Decision Processes 97, 117.

Chu Z., Gianvecchio S., Wang H. (2018) *Bot or Human? A Behavior-Based Online Bot Detection System*. In: Samarati P., Ray I., Ray I. (eds) From Database to Cyber Security. Lecture Notes in Computer Science, vol 11170. Springer, Cham. https://doi.org/10.1007/978-3-030-04834-1_21

Cressey, D. R. (1953). *Other People's Money: A Study of the Social Psychology of Embezzlement*. Montclair, NJ: Patterson Smith Publishing Corporation.

Davis, M. V., & Harris, D. (2020). *Strategies to Prevent and Detect Occupational Fraud in Small Retail Businesses*. International Journal of Applied Management and Technology, 19(1). https://doi.org/10.5590/IJAMT.2020.19.1.04

Deepak S., Anurag S., Mohit S. (2021). *Deep Transfer Learning Framework for the Identification of Malicious Activities to Combat Cyberattack, Future Generation Computer Systems,* Volume 125, 687-697, https://doi.org/10.1016/j.future.2021.07.015.

Del Mar Roldán-García M, García-Nieto J, Aldana-Montes JF. (2017). *Enhancing Semantic Consistency in Anti-Fraud Rule-Based Expert Systems. Expert Systems with Applications*. 90. 332–343 DOI 10.1016/j.eswa.2017.08.036

Dellaportas, S. (2012). *Conversations With Inmate Accountants: Motivation, Opportunity, and the Fraud Triangle.* Accounting Forum, 37, 29–39. https://doi.org/10.1016/j.accfor.2012.09.003

Discenza, R. & Forman, J. B. (2007). *Seven Causes of Project Failure: How to Recognize Them and How to Initiate Project Recovery*. Paper presented at PMI® Global Congress 2007—North America, Atlanta, GA. Newtown Square, PA: Project Management Institute.

Dorminey, J., Fleming, A. S., Kranacher, M.-J., & Riley, Richard A., Jr. (2012). *The Evolution of Fraud Theory*. Issues in Accounting Education, 27(2), 555–579. https://doi.org/10.2308/iace-50131

Duffield, G., & Grabosky, P. (2001). *The Psychology of Fraud. Trends and Issues in Crime and Criminal Justice / Australian Institute of Criminology*, (199), 1–6. https://search.informit.org/doi/10.3316/agispt.20013757

Durmic, N. (2020). *Factors Influencing Project Success: A Qualitative Research.* TEM Journal, 9(3), 1011–1020. https://doi.org/10.18421/TEM93-24

Economou, E., Kyriazis, N. (2017). *The Emergence and the Evolution of Property Rights in Ancient Greece*. Journal of Institutional Economics, 13(1), 53-77. doi:10.1017/S1744137416000205

Eryanto, D. (2020). *An Effective Anti-Fraud Program: How Do We Know? (The Challenge of Finding nn Anti-Fraud Program in the Indonesian Public Sectors)*. Asia Pacific Fraud Journal. 5. 288. 10.21532/Apfjournal.V5i2.157.

Fang, W., Li, X., Zhou, P., Yan, J., Jiang, D., & Zhou, T. (2021). *Deep Learning Anti-Fraud Model for Internet Loan: Where We Are Going*. IEEE Access, 9, 9777-9784.

Frankel, T. (2012). *The Ponzi Scheme Puzzle (Electronic Resource): A History and Analysis of Con Artists and Victims* (p. 1). New York: Oxford University Press.

Guo, C., Wang, H., Dai, H.-N., Cheng, S., & Wang, T. (2018). *Fraud Risk Monitoring System for E-Banking Transactions.* Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00030

Guo, J. X. (2019). *Measuring Information System Project Success through a Software-Assisted Qualitative Content Analysis.* Information Technology and Libraries, 38(1), 53–70. https://doi.org/10.6017/ital.v38i1.10603

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). *The risk of financial fraud: a management perspective.* Journal of Financial Crime. 1143-1159.

Holtfreter, K. (2015). *General Theory, Gender-Specific Theory, and White-Collar Crime.* Journal of Financial Crime, 22, 422–431. https://doi.org/10.1108/JFC-12-2014-0062

Jianhao, Y. (2019). *Design and Implementation of Bank Wind Control Anti-fraud Project Based on Big Data Technology.* In Journal of Physics: Conference Series (Vol. 1345, No. 2, p. 022064). IOP Publishing.

Lithuanian Banks Association. (2021*). "Elektroninių sukčiavimų mastas Lietuvoje per pandemiją išaugo kartais".* https://www.lba.lt/lt/naujienos/elektroniniu-sukciavimu-mastas-lietuvoje-per-pandemija-isaugo-kartais

Mackevičius J., Giriūnas L. (2013). *Transformational Research of The Fraud Triangle.* Ekonomika - Vilniaus Universitetas, 92(4). https://doi.org/10.15388/Ekon.2013.0.2336

Kim, B.-J., Kim, M.-J., Kim, T.-H. (2021). *""The Power of Ethical Leadership": The Influence of Corporate Social Responsibility on Creativity, the Mediating Function of Psychological Safety, and the Moderating Role of Ethical Leadership."* International Journal of Environmental Research and Public Health, 18(6), 2968. https://doi.org/10.3390/ijerph18062968

Kolomeets M., Chechulin A., Kotenko I., (2021). *Bot Detection by Friends Graph in Social Networks.*, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(2):141–159.

Kumar, U., & Gambhir, S. (2018). *Device Fingerprint and Mobile Agent Based Authentication Technique in Wireless Networks.* Int J Fut Gen Comm Netw, 11(3), 33-48.

Kurshan, E., & Shen, H. (2021). *Graph Computing for Financial Crime and Fraud Detection: Trends, Challenges and Outlook.* https://virtualibiblioteka.vu.lt/permalink/f/1ferss/TN_cdi_arxiv_primary_2103_03227

Kutz, G.D. (2006). *Framework for Fraud Prevention, Detection, and Prosecution.* United States Government Accountability Office, Washington, DC, 12 July.

Louzada, F., & Ara, A. (2012). *Bagging K-Dependence Probabilistic Networks: An Alternative Powerful Fraud Detection Tool. Expert Systems with Applications*. 39(14), 11583-11592

Mangala, D., & Kumari, P. (2017). *Auditors' Perceptions of the Effectiveness of Fraud Prevention and Detection Methods.* Indian Journal of Corporate Governance, 10(2), 118–142. https://doi.org/10.1177/0974686217738683

Meinert, M. C. (2016). *In The Fight Against Fraud, Strong Leadership is Key*. American Bankers Association. ABA Banking Journal, 108(2), 55.

Mulcahy, R. (2016). *PM crash course. A Revolutionary Guide to What Really Matters When Managing Projects.*

Neverauskas, B., Bakinaite, L., & Meiliene, E. (2013). *Contemporary approach to the possibility of project's success increase.* Economics and management, 18(4), 829-836.

Nugroho, I. S. (2019). *Does Leadership Really Matter in Combating Fraud? Indonesian's Millennials Perspectives.* Asia Pacific Fraud Journal, 3(2), 189-200.

Orso, A. (2010). *Monitoring, Analysis, and Testing of Deployed Software. In Proceedings of the FSE/SDP Workshop on Future of Software Engineering Research*. 263-268.

Piper, J., Metcalfe, A., (2020) *Economic Crime in a Digital Age*, Ernst & Young Report

PricewaterhouseCoopers. (2020). *Fighting Fraud: A Never-Ending Battle. PwC's Global Economic Crime and Fraud Survey*. https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

Project Management Institute. (2017). *Success Rates Rise: Transforming the high cost of low performance*. Pulse of the Profession 2017. 11. https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2017.pdf

Prostejovska, Z., & Tomankova, J. (2017). *Project Management: How to Assess a Project's Success.* Business & IT (Praha, On-Line), VII (1), 2–7. https://doi.org/10.14311/bit.2017.01.01

Puiu, M., (2014). *A Review of Antifraud Software Market. In Identities in Metamorphosis.* Literature, Discourse and Multicultural Dialogue. Section: Literature. Arhipelag XXI Press. 139-146.

Ramadhan, D. (2020). Root Cause Analysis Using Fraud Pentagon Theory Approach (A Conceptual Framework). Asia Pacific Fraud Journal, 5(1), 118-125.

Rockart, J. F. and Bullen, C. V. (1981), *A Primer on Critical Success Factors*, working paper no. 69, Center for Information Systems Research, Sloan School of Management, MIT. https://dspace.mit.edu/bitstream/handle/1721.1/1988/SWP-1220-08368993-CISR-069.pdf?sequen

Roseline, E. (2019). *Restoring the Capacity of Leadership as Role Model to Build Anti-Fraud Culture and System: A Study of Indonesia*. Asia Pacific Fraud Journal, 4(2), 167-175.

Rupšienė, L. (2007). *Kokybinio tyrimo duomenų rinkimo metodologija: metodinė knyga* (p. 147). Klaipėdos universiteto leidykla.

Sorunke, O.A. (2016): *Personal Ethics and Fraudster Motivation: The Missing Link in Fraud Triangle and Fraud Diamond Theories.* International Journal of Academic Research in Business and Social Sciences. Vol. 6, 159-164

Stamler, R. T., Marschdorf, H. J., Possamai, M., (2016). *Fraud Prevention and Detection– Warning Signs and the Red Flag System*

The Association of Certified Fraud Examiners, Grant Thornton LCC, (2021). *The Next Normal: Preparing for a Post-Pandemic Fraud Landscape*. https://www.acfe.com/uploadedFiles/ACFE_Website/Content/covid19/Covid-19-Preparing-for-a-Post-Pandemic-Fraud-Landscape.pdf

The Cambridge Dictionary. (2021). https://dictionary.cambridge.org/dictionary/english/fraud

Thonnard, O., Dabbabi, Z., Mironescu, M., Fontanes, D. (2018). *Reinforcing Application Security through User Behavioural Analysis.*

U.S. Government Accountability Office (GAO). (2015). *Framework for Managing Fraud Risks in Federal Programs.* https://www.gao.gov/assets/gao-15-593sp.pdf

Van Der Westhuizen, D., Fitzgerald, E. P. (2005). *Defining and measuring project success.* In Proceedings of the European Conference on IS Management, Leadership and Goverance 2005 (p. 157-163). Academic Conferences Limited.

Videnovic, S.D., Hanic, A.M., (2021) *Internal Fraud Committed by Employees in Insurance Sector*. http://tokoviosiguranja.edu.rs/wp-content/uploads/2021/07/21-02_3e.pdf

Wedge, R., Kanter, J. M., Rubio, S. M., Perez, S. I., & Veeramachaneni, K. (2017). *Solving the "false positives" problem in fraud prediction.*

Wilhelm, W.K. (2004). *The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management*. Journal of Economic Crime Management, Vol. 2 No. 2, p. 1-38.

Wolfe, D. T., & Hermanson, D. R. (2004). *The Fraud Diamond: Considering the Four Elements of Fraud.* The CPA Journal, 74(12), 38.

Yong, Y. C., & Mustaffa, N. E. (2017). *Critical Success Factors for Malaysian Construction Projects:* An Investigative Review. International Journal of Built Environment and Sustainability, 4(2). https://doi.org/10.11113/ijbes.v4.n2.180

ANNEXES

Annex 1

Qualitative research interview questions.

General questions:

1. Please choose the number of years of work experience you have.
2. What was your role in the project?
3. How can you evaluate your experience with other software implementation projects?
4. How does the project for anti-fraud tool implementation differs from other projects you've worked on?

Questions regarding anti-fraud tool implementation. Please choose one anti-fraud tool implementation project and respond to the questions regarding it.

5. How did the organization choose the tool that was implemented?
6. How would you evaluate the success of this project's implementation?
7. Which characteristics, in your opinion, characterize a project as successful or unsuccessful?
8. What types of challenges have you encountered while working to implement anti-fraud tool?
9. Which were the most difficult challenges?
10. How would you assess Top Management's overall commitment and attention to this project?
11. Would you agree that the organization that installed the anti-fraud solution regarded this project as a high priority?
12. How can you assess the Fraud Team's qualifications and participation in the project?
13. How can you evaluate the Software Suppliers' involvement, communication, and support during the project?
14. What, in your opinion, might be the cause of anti-fraud tool project failures? Postpones?
15. How essential do you believe it is that the organization with whom you worked on the anti-fraud tool implementation project follows and supports an ethical leadership style? Should such a company have a sense of social responsibility, and how can this be measured?

Professional opinion:

16. What are the most important takeaways or lessons learned from the anti-fraud software implementation project?

17. What advice would you provide to project managers who are working on anti-fraud software implementation projects?
18. What are the main differences between a conventional project and an anti-fraud software implementation project, in your opinion?

Qualitative research interview responses.

Table 9. Experts' responses to questions 1-3.

Expert	Question 1	Question 2	Question 3
Expert 1	*6-10 years*	*Fraud Manager*	*Not many projects. Usually, the ones related to fraud program*
Expert 2	*6-10 years*	*Business Analyst/Product Owner*	*I am responsible to build the product/ working software.*
Expert 3	*6-10 years*	*Software Developer - Testing*	*I had several different projects and with each of them I had shared different experiences which was truly helpful to me to understand key aspects of different products.*
Expert 4	*6-10 years*	*Fraud Prevention Analyst*	*As experienced in Face to Face and Non face to face fraud I can analyze the incoming fraud*
Expert 5	*11-15 years*	*Software Architect, Lead Engineer (Software provider)*	*I've been working on many systems of varying complexity in different roles.*
Expert 6	*11-15 years*	*Project Leader*	*Advanced to Expert*
Expert 7	*6-10 years*	*AML Compliance Expert*	*Mostly been working advisor to product owners and IT specialists*
Expert 8	*0-5 years*	*Specialist (Fraud team)*	*Upper intermediate*
Expert 9	*6-10 years*	*Project Manager*	*Very valuable experience that taught me what kind of information can be collected and misused.*
Expert 10	*0-5 years*	*Specialist (Software provider)*	*I was participating in several anti-fraud tool implementation projects.*
Expert 11	*6-10 years*	*IT Support (Software provider)*	*This is my main responsibility to implement anti-fraud technologies. I have plenty of experience.*
Expert 12	*6-10 years*	*Fraud Manager*	*Small experience*

Table 10. Experts' responses to questions 4-6.

Expert	Question 4	Question 5	Question 6
Expert 1	*Mostly I have worked on Fraud projects. Cannot compare with other type.*	*I was reviewing couple of tools. In the end I decided to test one of those. And results were satisfying*	*The current project is still ongoing. Far from now it looks to be promising.*
Expert 2	*The tool has many legal requirements, which should be fulfilled. And one of the key departments is `compliance team.*	*It was based on FSA requirements to have particular level of security and knowledge about the customers.*	*The project was successful as the company managed to comply with requirements and software was built on time with good quality.*
Expert 3	*I have been working on several projects that needed to implement anti-fraud tools. The experience itself was really interesting and different from my other experiences, because each tool is related to the processes that are carried with principle - here and now, as well as that the project and tool itself can change even in the course of implementation. The legal framework and the global features of fraud, forced us to adapt projects to today's needs and to look forward to a rapidly changing environment.*	*Organization was simply interested in highest quality tool on the market, so that was top priority for choosing particular tools*	*Implementation was great success, because tool was quite easy to handle*
Expert 4	*In previous projects, I worked on data related to fraud to minimize the risk. Fraud related projects have higher amount of transparency.*	*First, they tried to test the given project and match the result with the previous data*	*Project was successful, it increased its limits and reduced SLA's.*
Expert 5	*The legal requirements are stricter. Mistakes in software design or simple bugs might cause legal troubles.*	*The organization was choosing from several POC from various providers to select the strategic partner.*	*Limited success. The project was understaffed during the development and due to changes in priorities got sidelined.*
Expert 6	*Different scope and different regulatory environment.*	*There was market analysis and research.*	*100% success.*

Expert 7	*It seemed to more complex as expert level legal knowledge was compulsory, and many teams were involved*	*By comparing several existing tools, their advantages, and disadvantages*	*Really successful, everyday tasks are completed faster, more processes were automated, but several updates after implementation were still needed*
Expert 8	*Have more safety as security restrictions*	*Trial periods*	*Successful*
Expert 9	*It helps identify various ways how to misuse data and where to be careful.*	*Through market research*	*Project was not successful and wasn't finished when I left the company.*
Expert 10	*Almost impossible to create universal project, because every fraud type, even place, where fraud is issued, have many exceptions*	*It was tested, then released and later on had some changes*	*Pretty good.*
Expert 11	*The increased involvement of the people who are receiving the anti-fraud software.*	*The tool was selected based on price and tested on the company use case.*	*It was successful*
Expert 12	*This project requires certain skills, the tool is complicated*	*It was pretesting phase*	*Not successful*

Table 11. Experts' responses to questions 7-9.

Expert	**Question 7**	**Question 8**	**Question 9**
Expert 1	*If the tool is functioning and catches fraud. Less false positives. More true positives. The prevented fraud losses should be higher than the spendings on the tool. And also, it should comply with legal/audit requirements.*	*IT resources. IT infrastructure in my organization. It is quite hard to build powerful anti-fraud engine, when we are not simply collecting many Datapoints from our clients. We simply cannot use full functionality of the tool.*	*Our IT infrastructure shortages.*
Expert 2	*They key metric for this product/ project was "how close we are to reach FSA target for particular question".*	*One of big challenges was to convince other employees to use the program and to help building the product. As well it was hard to collect requirements from*	*They main challenge was related with constantly changing legal requirements for particular question, e.g. Every 3-6 months.*

		different sources and find the right data in order to make data driven decisions.	
Expert 3	*In my opinion, the most important thing to understand that the project was successful are quick feedback from colleagues, and the obvious increase of productivity and quality after project implementation*	*The most difficult thing was the technical side of the project, because the technical side needed to be brought into line with existing laws and global practice*	*As I mentioned above, technical implementation and technical decisions how to make project implement and make it most efficient*
Expert 4	*Project is successful when it's reduces the risk of fraud and also prevent the financial loss.*	*Fees, security of the company as well card holder, time, insights*	*Security, time*
Expert 5	*Success could be an integration to daily operations (maybe even as a shadow system), and having a never-ending backlog of fraud scenarios to handle.*	*Usually, the natural language understanding part is challenging. Also, the system is open-ended, meaning that new cases appear as time goes on.*	*Shift in priorities for the project.*
Expert 6	*Meeting all the initially planned and subsequently added goals and objectives.*	*Successful tool integration and addressing of unexpected new variables.*	*The proper addressing of unexpected new variables faced during the implementation.*
Expert 7	*Mostly by reviews of everyday users*	*Miscommunication*	*Most significant- complying with the regulations and communication with IT teams*
Expert 8	*Usability adaptability*	*Errors and reliability*	*Information and communication between departments*
Expert 9	*If it fulfills the preset goals*	*Mainly data analysis, to differentiate data coming from different systems and their categorization*	*Various environments in the company*
Expert 10	*If set goals are reached, then project is successful.*	*I had to weigh potential risks, identify areas that might disturb to implement the tool successfully.*	*Hardest part is to clarify the vision how tool should work and look.*
Expert 11	*It performed well and as anticipated thus successful*	*People do not like changes, so it was hard to prove them, that the tool will be valuable.*	*Training*

Expert 12	*Project delivers the value, stakeholders' satisfaction, and overall satisfying results.*	*There was miscommunication, there were lack of resources, low prioritization in the management*	*IT resources*

Table 13. Experts' responses to questions 10-12.

Expert	**Question 10**	**Question 11**	**Question 12**
Expert 1	*Top management are supportive from the beginning. They understand the need for the tool and fraud program itself. Even we had problems with IT resources, it was way much better than other projects which were not prioritized.*	*Yes*	*I cannot evaluate myself. I think I am committed and am involved in all process.*
Expert 2	*Top Management was super interested in the project as we needed to comply with FSA or the fines would come.*	*Yes*	*Fraud team was consulted during the development of the product.*
Expert 3	*Top management has been heavily involved in both product development and its implementation, also testing and use of it*	*Yes, because organization operates with in business field which is highly involved in anti-fraud management*	*By their experience and skill set*
Expert 4	*First, I will try to give overview of project and showcase its functions, also I'll high the points to get better result*	*Yes, I agree*	*Excellent*
Expert 5	*High commitment and attention initially which, unfortunately, gradually wears off.*	*At first it was, but when it was "useful" the priorities shifted despite the fact that the backlog was far from being empty.*	*It was somewhat hard to get to the Fraud team. The fact they resided in a different country didn't help.*
Expert 6	*Excellent*	*Yes*	*They did a good job advising other teams and made sure everything is as in regulator's recommendations.*
Expert 7	*Top management was strongly involved*	*Yes*	*Very inclusive*

Expert 8	*Helpful and prompt*	*Yes*	*Fraud team was fully involved and had appropriate qualifications.*
Expert 9	*It was always on a top priority list.*	*Mostly yes*	*Various environments in the company*
Expert 10	*Not much attention was given. Analysts were more oriented to evaluate the tool.*	*Organization expected to receive a good tool, but it didn't give enough support and sources that might help.*	*Some people had 3+ years' experience, but they didn't want to be involved very much.*
Expert 11	*Encouraging as well as they were on top of things to make it happen*	*Yes, I would*	*Based on feedback, they were performing.*
Expert 12	*Non-permanent commitment. Low prioritization, and less attention overall.*	*No, it wasn't a priority.*	*The team has high commitment, cannot comment on qualifications.*

Table 14. Experts' responses to questions 13-15.

Expert	**Question 13**	**Question 14**	**Question 15**
Expert 1	*Good. I'm not satisfied, that we do not have exact people assigned to us, and each time we have new developers on the call. However, all agreement signing process was fluent and now we are getting answers to all our questions.*	*Lack of resources, and low priority for the project. As well as no ownership. It also might be, that the tool which was selected is simply not working for the company – do not provide expected results.*	*Ethical leadership is important. I think, that if company is trying to hide some fraud losses or are scared to see the real level of fraud they have – those projects will never succeed, there will be less attention for projects.*
Expert 2	*I was working as that: supplied information how to use the product and helped to solve all the problems with the system.*	*The complexity of the system, which correlates with development time. Successful onboarding of the employees like how they are using the system.*	*The leadership commitment is required in such projects, otherwise it won't be funded.*
Expert 3	*Software suppliers were always available, and you could always expect to get fast and quality feedback from them*	*Lack of qualified testers and lack of involvement of management*	
Expert 4	*By forming a team by their skill and then to aligned them in single channel.*	*By relaying on the same fraud pattern and the same prevention method, instead of looking into*	*I believe it is very essential for the organization to follows and supports an ethical leadership,*

		fraud with more criticism and complexity. This results in low quality of the tool.	*social responsibility is one the priority for every organization. We can measure it by feedback and positive response.*
Expert 5	*I was in the supplier position.*	*Shift in priorities. Over-ambitiousness initially which eventually will meet the reality, and this will cause disappointment.*	*It is important for the long-term success and partnership. No idea how to measure it.*
Expert 6	*Excellent*	*Wrong definition of the scope and the estimated costs.*	*I believe it is very critical in order to succeed at delivering transparent messages and clear goals communication. Yes, the company should have this sense of social responsibility measured through the strong alignment with different stakeholders and accurate tracking of effort/cost - benefit/value.*
Expert 7	*Strongly involved*	*Tool not being perfectly suitable for a certain organization*	
Expert 8	*Qualified*	*Error and data delays*	*Always*
Expert 9	*Very good*	*Data management, complicated architecture.*	*Each company should understand the social responsibility and have specific department in order to follow through.*
Expert 10	*From my side - I did my best. Other communication - responses, assistance - didn't come as soon as possible.*	*Not enough support from experienced colleagues, lack of support from organization.*	*Company not always showed ethical leadership style.*
Expert 11	*Based on the agreed SLA's, issue tickets and their resolution*	*Legal issues, internal policy alignment with the new tool, resource allocation as in employees and hardware etc.*	*It is very important, I would not like it any other way, the ethical leadership is a must. I am not sure, and I am having difficult time managing how it*

			could be measures, perhaps employee feedback
Expert 12	*They were fully involved and collaborative*	*Low attention from top-management, e.g., delivering resources. Unclear planning. Changing project managers, and team without distribution of tasks.*	*I think that my company do not follow ethical leadership style. I do not think that they are trying to hide something. But I think that my project would be more successful it we would be more transparent.*

Table 15. Experts' responses to questions 16-18.

Expert	**Question 16**	**Question 17**	**Question 18**
Expert 1	*Do not expect that people will do their best. You have to be involved in every part of the project. If you are the end user, please put your nose everywhere. Also, the results might be not so successful as you expected. And providers are very helpful when they want to sell, however when results are not good enough – they will blame on your weaknesses.*	*Try to understand every detail. Keep good communication. If project is not prioritized – leave it or fight for priority. There will be no resources* *And you will end up with trouble.*	*Cannot exactly compare, but I think, that fraud projects have more details, since it includes and tracks a lot of different systems and client actions. It can be more complicated. As well as it is using sensitive data and should be carried out with high confidentiality.*
Expert 2	*The most important part is to get everybody onboard: that all organization would want to use the tool and that all the organization would trust that system and would be willing to provide feedback for further developments.*	*Good luck. Or try to get green light from top management and all other managers.*	*ROI*
Expert 3	*Most important lesson I've learned was that patience and hard work could move the mountains*	*Be patient, be curious and be open minded to various opinions*	

Expert 4	*Reporting procedures, Corrective action, Quality assurance, On-going monitoring*	*Preventing fraud is far preferable to detecting it after the fact. In practice, the same systems and controls established to prevent fraud may help in detecting it*	*It builds organisation from inside also it helps to build trust prevent the threats*
Expert 5	*Manage the complexity and keep the rate of delivery, set-up an evaluation framework early on.*	*Start super small, nanoscale, then grow your ambition.*	*Anti-fraud projects are way more open-ended than "conventional" projects.*
Expert 6	*Proper inclusion of all relevant stakeholders and following an agile approach.*	*Start with a very clear definition of the scope and expected outcomes collected from all relevant stakeholders.*	*The higher frequency of facing unexpected new variables.*
Expert 7	*Teamwork makes the dream work.*	*Pick as many as possible tools for initial review*	*More teams are involved than usually*
Expert 8	*Patience*	*Being agile*	*Data security and relatability*
Expert 9	*That planning and data management is very important*	*Be clear on what data you need and what needs to be done with it*	*Mainly the end goal.*
Expert 10	*It should be a team that would work on such projects. Different experience and suggestions might help to avoid more risks of failure.*	*Ask for more advice, support and follow up from colleagues and organization.*	*Don't have an explanation.*
Expert 11	*It takes time and thing do not always go as planned*	*Communication to give information and receive feedback*	*The increased involvement of the people who are receiving the anti-fraud software*
Expert 12	*That project is hard to handle, that you need to plan and communicate constantly. That you should fight for resources, or if there are no Resources -then do not initiate the project.*	*Understand the leadership role position in the project. If they do not support fraud culture- do not start the project. It will be hard. Take responsibility, fight for resources. Report to top management if you struggle.*	*It depends on project, but might be, that prioritization can be the difference. Fraud management projects not usually have high prioritization*