STRATEGIES AND INTERNAL CONTROL PROCEDURES FOR DECREASING FRAUD IN FAITH-BASED NONPROFIT ORGANIZATIONS

by

Shawn Miller

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

December 2021

Abstract

This study addressed the problem regarding the lack of strategies and internal controls in faith-based nonprofit organizations which resulted in a higher risk of fraud, waste of funds, or abuse of funds in charities, churches, and other related ministries. This risk was the result of trust by organizations that employees would not commit fraud and due to a lack of sufficient resources. This study specifically researched faith-based nonprofit organizations that are located in Texas. This qualitative case study included two faith-based nonprofit organizations located in or near Houston, Texas. The research found several themes including: frauds occur, segregation of duties, approval controls, review process, and policies and procedures. The study also found several internal controls, policies, and procedures that these organizations could implement to decrease the risk of fraud, such as a whistleblower policy, background checks, segregation of duties, review of financials, and limited access to accounting procedures. Further research could be conducted on the implementation of internal controls after a fraud was discovered and the restoration of donor trust.

Key words: fraud, nonprofit, faith-based, internal controls, accounting

Dedication

This work is dedicated to my wife Maria, our daughters, Mckensie and Makayla, and our son Noah for their moral, emotional, spiritual, and financial support throughout the entire period of the study. Through all of the challenges, they stood by me and encouraged me to continue to the finish line. I also dedicate this study to my father and mother who have always been so supportive of my goals and dreams including this one. And I dedicate this study to my Lord and Savior Jesus Christ for giving me the opportunity, strength, wisdom, and ability to finish this study.

Acknowledgments

I would like to acknowledge my professors who guided and assisted me through the doctoral journey. I would like to extend a special thanks to my Dissertation Chair, Dr. Darnell Huntley for her patience and commitment to seeing me through this process. I also want to acknowledge my high school bookkeeping instructor, Mr. Vankirk, who saw my spark of interest in accounting and helped set in motion what would eventually lead to the completion of this study.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Nonprofit organizations are important to the success of a society. These entities provide goods and services to the public that help those who are in need and those who are hurting. Protecting these organizations from fraud is an important factor needed for their continued success. This section of the study addressed the foundation of the study, which includes the background of the problem, the problem statement, and the purpose statement. This section also discussed the research questions, conceptual framework, and nature of the study. Definition of terms, assumptions, and delimitations were also explained; the reduction of gaps and the implications for Biblical integration were also discussed. The relationship to the field of study will also be explained followed by a review of the professional and academic literature. Subsequent sections discussed the research project and the application to professional practice and implementations for change.

Background of the Problem

Nonprofits organizations are not in the business of making a profit. Their goal is to provide a service to the community at a reduced rate, or for free, to benefit others. These organizations rely on donations, tax dollars, and sometimes the sale of items to raise funds for their cause. Since these organizations are not seeking to achieve profits, they are unable to raise the capital that large corporations are able to obtain through the sale of stock, initial public offerings, and other capital raising opportunities. As a result, nonprofit organizations do not have the same resources that are available to for-profit companies. This lack of resources leads to less spending on many different areas within the organization.

One area where nonprofits are unable to spend as much money as for-profit companies is in the area of salaries. Reduced salaries mean that the best employees will often be attracted to large for-profit corporations over nonprofit organizations. In addition, less resources may be spent on the management of the organization's resources, including the accounting department and the support of the accounting information system. Very small nonprofits such as churches and some charities may hire volunteers to manage the organization's finances. These employees may save the organization money by not requiring a salary; however, their level of experience may be less than that of a Certified Public Accountant (CPA). As a result, the internal controls of a nonprofit organization may not be as robust as those that are found in a for-profit company. The nonprofit may not have the resources to implement separation of duties and other internal controls that can protect an organization from fraud.

In addition, these volunteer employees are often placed in a position of trust where the organization believes that the employee would not steal from the charity because that person has the best interest of the organization in mind. This trust factor can provide the opportunity for unscrupulous employees or volunteers to take advantage of an organization's lack of internal controls. Committing a fraud was easier when controls were not in place to prevent and detect typical frauds.

Even after a fraud was committed, the nonprofit organization may feel hesitant to prosecute the employee. If a major fraud was made public by a nonprofit organization, many donors felt that trust was broken, and that they should no longer give to that organization. In addition, nonprofits may not prosecute because they do not have the financial means to hire lawyers and pay for an expensive lawsuit. Therefore, the perpetrator of the fraud has more opportunities to commit fraud within a nonprofit organization, and they have less chance of being punished when the scheme was discovered. These two issues have led to many frauds being committed against nonprofit organizations.

Problem Statement

The general problem addressed was the lack of strategies and internal controls in nonprofit organizations which resulted in a higher risk of fraud in charities, churches, and governmental entities. Baapogmah et al. (2015) found that ethics, accountability, and control mechanism were the major issues that nonprofits faced. They also discovered that these organizations struggle to implement controls due to a lack of sufficient resources. Harris et al. (2017) found that one-sixth of all major embezzlements occur within the nonprofit industry, and that nonprofits are susceptible to fraud because they rely on a culture of trust. Archambeault and Webber (2018) found that an estimated 5% of a nonprofit's revenues are lost each year due to fraud, and that nearly one-fourth of nonprofits do not survive three years after publicizing the fraud. The specific problem addressed was the lack of internal controls in faith-based nonprofit organizations within Texas resulting in a higher risk of fraud within those entities.

Purpose Statement

The purpose of this qualitative study was to add to the body of knowledge by expanding on the understanding of the factors that lead to frauds being committed in nonprofit organizations. This larger problem was explored through an in-depth study of strategies and internal controls that can help faith-based nonprofit organizations in Texas. These strategies and internal controls can be used to mitigate the risk of fraud within nonprofit organizations.

Nature of the Study

This section will discuss the methodology and design that were used in the research. The methodology can be qualitative, quantitative, or a combination of both, which is called mixed methods. There are several designs for research which include designs such as narrative, grounded theory, ethnography, and phenomenology.

Discussion of Method

The research method that was most appropriate for this research was the qualitative design using a multiple case study method. This was the most appropriate method because the qualitative design was used to gain insight into a problem and explore the depths of the issues related to the problem, which cannot be done with the quantitative method. A qualitative design was appropriate for this study since the qualitative design seeks to explain or understand the research questions (Creswell, 2015). Other studies have also used the qualitative design. Rockson (2019) conducted research on strategies for preventing fraud in church organizations in Ghana using the case study method. In this study a qualitative design was used via open-ended questions.

The research methodology is the method, at a high level, by which the research will be conducted. Research can be conducted using a fixed, or quantitative design, a flexible, or qualitative design, or a mixed approach that combines both qualitative and quantitative designs. The design that was selected will determine the types of methods that are used in the research. The quantitative design was not chosen for this research because the quantitative design does not help provide the depth of exploring the research questions, which can be better provided using the qualitative design.

Discussion of Design

This study was conducted with a flexible design using qualitative methods specifically, a multiple case study design was used. Since this study was seeking to explain or understand why fraud was committed in nonprofit organizations, a qualitative design was more appropriate than a quantitative design. The qualitative design helped to explain the research questions better than the quantitative design. Other studies have also used a case study method. Derby (2015) conducted a case study of charismatic churches in Ghana, which discovered the mismanagement of funds as a major challenge.

The case study was the most appropriate method because it is used to understand an instance of the problem that is being researched. The narrative method was not selected since this method is used to study the lives of individuals by obtaining stories about their lives (Riessman, 2008). The grounded theory method was not used because this design is used to derive a general theory, a process, action, or interaction grounded from the viewpoints of the participants; the ethnography method was not selected since this design is typically used to study a pattern of behaviors, language, and actions of a cultural group (Creswell, 2015). The phenomenology method was not chosen because this design is used to describe a phenomenon described by participants of a lived experience (Creswell, 2015).

The case study method was an appropriate method for this research. Gallagher and Radcliffe (2002) conducted research using a case study method on fraud related to nonprofits. Gregory (2017) also used a case study method to explore fraud within nonprofit organizations. Therefore, the case study method was preferred over other research methods.

Summary of the Nature of the Study

In summary, this research was conducted using the qualitative method with a multiple case study design. This approach provided the depth of understanding that was needed to better understand how fraud was committed in faith-based nonprofit organizations. Other studies also used a qualitative design with a case study method.

Research Questions

There were three major research questions that were used to address the problem statement. These questions attempted to discover why nonprofits are susceptible to misappropriations and how to prevent these frauds from occurring.

RQ1: What are the factors that can lead to increased risk of fraud, the waste of funds, or the abuse of funds within faith-based nonprofit organizations?

RQ2: What are the strategies and internal controls that faith-based nonprofits can implement to mitigate the risk of fraud, the waste of funds, or the abuse of funds?

RQ3: What are the strategies and internal controls that faith-based nonprofits in Texas can implement to mitigate the risk of fraud, the waste of funds, or the abuse of funds?

RQ1 sought to understand the factors that can increase the risk of fraud, the waste of funds, or the abuse of funds within nonprofit organizations. Understanding these factors was a key to being able to identify the internal control weaknesses that may make these organizations more vulnerable to fraud, waste, or abuse. It may also provide areas within the accounting department that need to be monitored with a higher level of scrutiny.

RQ2 considers the strategies that organizations can implement to reduce the risk of fraud, waste, or abuse. These strategies may include a use of internal controls and other tactics which may not completely eliminate the threat of fraud, waste, and abuse, but may be able to reduce that risk. These strategies will be weighed against the cost to implement, ensuring that the cost does not exceed the intended benefit.

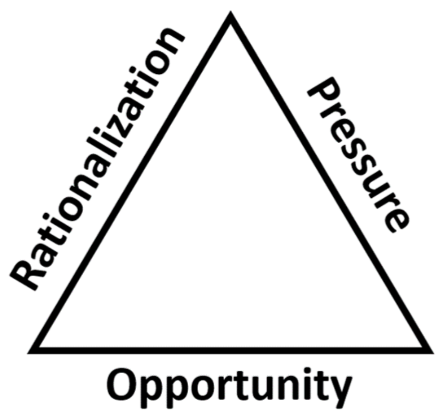
RQ3 identifies strategies that nonprofits can implement specific to those that are based in the state of Texas. This question will help to address the specific problem statement related to this research. These strategies may or may not differ from those strategies that nonprofits seek to implement in other organizations both domestically and globally.

Conceptual Framework

The conceptual framework for this study was the fraud triangle. This concept was originally developed by Cressey (1950) and includes three key elements that are present when fraud occurs. Figure 1 depicts the three aspects of the fraud triangle, which are pressure, rationalization, and opportunity (Kelly, 2017).

Figure 1

The Fraud Triangle



Source: Miller (2022)

Discussion of Pressure

The first leg of the triangle is labeled pressure, which is the motive that makes an individual believe that they have a financial problem that does not have a legitimate solution (Harris et al., 2017). Pressure can manifest in several forms. It can originate from having large personal debt, living beyond one’s means, greed, and addiction (Abdullahi & Mansor, 2018). Self-imposed financial hardships were found to be the most common motivation for committing fraud (Bonny et al., 2015). Kramer (2015) stated that almost all perpetrators of fraud spend their ill-gotten gains instead of saving it, which can be a red flag that an employee has committed fraud. For example, one Chief Executive Officer (CEO) perpetrated a fraud to pay for gambling on horse races (Lenz & Graycar, 2016). Pressure can also come from upper management, such as management requiring that the financial statements be altered to make the organization appear better financially (Albrecht et al., 2015).

Discussion of Rationalization

Second, there is rationalization, which allows the individual to morally justify the fraud and convince themselves that they are not acting immorally (Harris et al., 2017). Most people are able to rationalize or justify why they are committing a fraud so that they do not have to admit to themselves that they are doing something wrong. Rationalization can include phrases such as "I was just part of a team that was doing it…I can't see that it hurts anyone…I deserve more money…I fully intended to pay back the money that I took" (Free, 2015, pp. 184-185). These types of rationalization involve entitlement, displacing responsibility, miscontruing consequences, and moral justification (Free, 2015). Although some are able to rationalize the fraud, many still have an inner voice alerting them before committing the crime that what they are doing is wrong, and then giving them a guilty conscience afterwards that the action was unethical (Schuchter & Levi, 2015). Some claim that this inner voice becomes quieter over time as the fraud continues to be perpetrated (Schuchter & Levi, 2016).

Discussion of Opportunity

Opportunity is the third leg of the triangle. The opportunity for a fraudster to commit a crime increases the risk that a fraud could happen. Without opportunity fraud cannot occur (Marks & Ugo, 2020). There are two aspects of opportunity which are susceptibility to manipulation, and the conditions that may allow a fraud to occur (Marks & Ugo, 2020). The first two legs of the triangle, pressure and rationalization, are factors that an organization does not have significant control over. The third leg, opportunity, is the area that organizations can control through internal controls and other strategies (Harris et al., 2017).

Discussion of Relation to Study

The fraud triangle is related to this study because it can be used to understand why fraud occurs within organizations. Understanding why fraud occurs can help organizations develop internal controls to detect and prevent fraud in the future. This framework addresses the research questions by studying the elements that lead to fraud. Assessing an organization's risk for fraud will answer the first (RQ1) research question. Developing control activities will answer the second (RQ2) and third (RQ3) research questions. This study led to the discovery of several internal control themes and strategies that nonprofit organizations can use to reduce the risk of fraud.

The findings from this study also reinforce the conceptual framework. The major fraud that was discovered in one of the nonprofit organizations was based primarily on opportunity. The employee at the organization was able to perpetrate the fraud because he had the opportunity to do so. The lack of oversight for this employee, and the trust that the organization had for this individual, prevented typical internal controls from operating properly. If the standard controls were in place, this individual may not have had the opportunity to commit the fraud that he perpetrated over a period of several years.

Discussion of Relationships Between Concepts

Each of the elements of the fraud triangle help organizations understand how frauds are committed. Homer (2020) conducted a systematic review of 33 empirical studies on the fraud triangle. Homer (2020) found that 32 of the studies supported at least one element of the fraud triangle and that 27 supported all three elements. There is general support for the fraud triangle theory across different industries and countries (Homer, 2020). Omar et al. (2016) found that fraud committed at an organization was based on the opportunity element, due to a lack of internal controls, as well as lifestyle and financial pressures on the perpetrators.

Summary of the Conceptual Framework

The conceptual framework was based on the fraud triangle. This theory states that the three elements of fraud includes pressure, rationalization, and opportunity. By understanding this framework organizations are able to design internal controls and other strategies to detect and prevent fraud.

Definition of Terms

Charities: For the purpose of this study these are organizations that have nonprofit 501(c)(3) status with the Internal Revenue Service (Helge, 2017). These organizations are exempt from paying federal income taxes and can collect tax-deductible contributions from donors (Helge, 2017). Their purpose is not to generate a profit for shareholders nor owners, but to provide a service that will benefit part or all of society (Helge, 2017).

Faith-based Organization: For the purpose of this study this is an organization that engages in humanitarian work generally with a religious motivation (Azmat et al., 2019). These organizations often have strong ties with other religious organizations, share common values with those entities, or may receive funding from those organizations (Azmat et al., 2019).

Financial Administrator: For the purpose of this study this is any employee who has access or oversight of the financial records or financial assets of the organization such as managing the budget or preparing financial reports (Hughes, 2018). This role may include only one employee in smaller organizations, or numerous staff and mangers in larger organizations (Hughes, 2018).

Fraud: For the purpose of this study fraud is defined as the intentional practice of deceiving or misrepresenting the truth for the purpose of causing injury or depriving another of their right (Omar et al., 2016). Fraud must be intentional, otherwise it may fall under the category of negligence. This could occur if an employee makes a mistake or error from being careless (Zahra et al., 2005).

Internal Controls: For the purpose of this study internal controls are plans used by an organization to safeguard the assets and ensure accuracy of the financial information (Chen et al., 2017). These plans can take the form of policies, procedures, rules, and other methods to ensure compliance with the plans that are to be followed within the organization (Nawawi & Salin, 2018).

Nonprofit Organization: For the purpose of this study these are organizations that support a variety of causes such as religious, educational, scientific, humanitarian, and environmental, and operate without shareholders or a profit motivation (Meckstroth & Arnsberger, 1998). These organizations may or may not have 501(c)(3) status with the Internal Revenue Service (Leland, 1996).

Assumptions, Limitations, Delimitations

Assumptions, limitations, and delimitations are discussed to clarify the scope of the research. Assumptions are needed to conduct research efficiently and effectively, and in areas where research cannot be conducted (Bloomberg & Volpe, 2012). Limitations are inherent in areas where the researcher does not have control of the variables, and delimitations are needed to properly limit the scope of the research (Bloomberg & Volpe, 2012). These three concepts help to establish the scope of the research.

Assumptions

Assumptions are conditions that the researcher takes for granted (Leedy & Ormrod, 2019). For purposes of this study it was assumed that the participants in this study were truthful and honest in their responses within a normal level of variance (Harmon, 2011). It was also assumed that the participants were willing to share the internal controls that they used to mitigate the risk of fraud so that others might benefit from their responses (García-Sánchez et al., 2019). It was further assumed that the controls that were implemented by the participants will be useful for other nonprofit organizations in helping to prevent fraud in their organizations (Hoos & Bollmann, 2012). In addition, it was assumed that certain generalization can be made based on the factors that were discovered through this study (Nørreklit et al., 2016).

Limitations

Limitations are those factors that the researcher does not have control of and could affect the results of the study (Baron, 2008). This study was limited in that respondents may not fully know the answer to the questions or be knowledgeable about all the internal controls within the organization. This limitation was mitigated by interviewing those that are most knowledgeable about the organization's controls. In addition, some respondents may provide limited response for fear that sharing any weaknesses in their organization may draw negative attention to their organization. This limitation was mitigated by ensuring the respondents that confidential information would not be disclosed with the organization's name. Furthermore, there may be limitations between what the respondents communicate that they do, and what they actually do. For example, an organization may state that they require two signatures on a check, when most checks are signed with only one signature. This limitation was mitigated by finding collaborative information where possible. In addition, the information gathered from the respondents may contain information that cannot be independently verified; in these cases, the researcher will have to rely on the honesty and accuracy of the respondents' answers. This study was also limited in the responses that were received due to the current COVID-19 environment that the world is facing. Some organizations may not have wanted to participate in the research due to these factors. This limitation was mitigated by providing safe alternative means of collecting information, which involved social distancing.

Delimitations

Delimitations are factors that the researcher has some level of control over which helps to set limits for the research (Baron, 2008). Due to the large number of nonprofit organizations that are operating throughout the world, this study delimits the research to two nonprofits that are in the Houston and surrounding urban areas in the state of Texas within the United States. This study was further delimited by only researching those nonprofit organizations which are faith-based and use their beliefs as a contributing factor to their organization's mission.

Significance of the Study

The significance of this study was to understand the specific internal control weaknesses at a faith-based organization. Understanding the factors that contribute to fraud within the nonprofit organization is important to understanding how to prevent future frauds at that organization from occurring. By understanding these factors, steps can be implemented to reduce these issues which cause the organization to be at an increased risk of fraud. By identifying and addressing these factors, the nonprofit can mitigate their risk of loss, and have resources available for their intended usage. Preventing more frauds from taking place will help to increase the trust of donors and other contributors that the resources of the organization are safe and secure. A better protected nonprofit organization will benefit society with a better operated charity, and better equipped employees to work at that organization.

In addition, fewer resources will be wasted by fraudsters who misuse the organization's resources, based on one or more of the identified factors. This savings will benefit the nonprofit as well as the people they serve, which will result in the organization being able to be better manage their resources. Therefore, better understanding the factors that lead to fraud can have a significant impact on both the nonprofit and society. These findings could also be applied to other faith-based nonprofit organizations to help detect and prevent fraud from occurring.

Reduction of Gaps

This study attempted to reduce the gaps that exist in the current literature. Nonprofit organizations tend to have fewer resources available to them than for profit corporations, which results in less resources for internal control strategies. This research attempted to find strategies and controls that faith-based nonprofits can implement, even with limited resources, to ensure that the assets and accounting information systems within the organization are protected and secured. There is limited research on strategies that faith-based organizations can adopt, and therefore this study attempted to reduce those gaps and provide strategies that will benefit those organizations.

Implications for Biblical Integration

Having a Biblical perspective when conducting research is important to Christians, but it also benefits other as well. Both Christians and non-Christians agree that implementing concepts such as integrity, objectivity, and trust are attributes that help support good research. These and other concepts can help in conducting research in the field of business.

Conducting business research from a Biblical perspective involves approaching research from a Biblical worldview. Wilkinson (2005) stated that this means that the standard of whether something is true is based on whether it is consistent with the Scriptures. The Bible is the measuring stick by which research is conducted. By studying the world through the lens of the Bible, researchers can gain knowledge (Wilkinson, 2005). For example, a Christian researcher can start with the reality that humanity lives in a fallen world, and therefore they should expect certain types of behaviors to dominate in the business world. Greed, selfishness, and fraud should not surprise the Christian researcher, due to his understanding of man's sin nature.

In addition, Christianity provides a basis for normative research and prescriptive statements (Wilkinson, 2005). Normative research is research on how things should be done. The secular world often is unable to make a value judgment because people cannot agree as to what is right or wrong. However, the Bible provides a standard for right and wrong, which provides a means to conduct normative research.

The Christian perspective can be used in research using a variety of methodologies and research types, while still applying biblical truth to the accounting profession (Wilkinson, 2005). For example, one article noted that Christian researchers in accounting have ample opportunities to conduct research on corporate governance, social and environmental accounting, and tax compliance (Wilkinson, 2005). These areas of research could benefit from a biblical perspective because the results would show how people acted unethically as compared to the biblical standard.

In addition, research should be conducted with diligence and due care. These attributes are in line with Biblical principles. The Bible says that, "whatever you do, work at it with all your heart, as working for the Lord, not for human masters" (Colossians 3:23, *New International*

Version, 1973). Consequently, researchers should conduct research as if it is being conducted for God, and not just for a university or for a degree.

The Bible also speaks to how research should be conducted. 1 Thessalonians 5:21 says, "but examine everything carefully; hold fast to that which is good" (*New American Standard Version,* 1960). Research should be conducted with due care and diligence. Evidence should be examined carefully so that proper conclusions can be made. This research will attempt to meet those expectations and ensure that proper examination of the evidence was used to study the strategies for decreasing fraud in nonprofit organizations.

The research of this topic was also consistent with Biblical principles. Since the problem statement addresses strategies for decreasing fraud in nonprofit organizations, there are passages that emphasize the importance of these concepts in business. For instance, the Bible speaks against fraud and dishonesty in several passages. One such passage is Deuteronomy 25:15 (*Christian Standard Bible,* 2017), which says "You must have a full and honest weight, a full and honest dry measure, so that you may live long in the land the LORD your God is giving you." Proverbs 11:1 (*CSB*, 2017) echoes this passage by saying, "Dishonest scales are detestable to the LORD, but an accurate weight is his delight." These passages are referring to weights that were used in ancient times to weigh an item on a scale. God does not want people to use weights that are designed to deceive customers into thinking they are getting more than they are receiving.

For example, in California people can go to the recycling center to receive money for aluminum cans. A dishonest recycling center might try to say that a customer only brought in 200 pounds of aluminum, when they had 250 pounds. Conversely, a customer might try to deceive the recycling center by filling some empty aluminum cans with concrete. Both situations are examples of dishonest scales. This is what the passage above is referring to when it says to use honest weights. The weight does not have to be a physical weight; it could also be referring to a monetary weight.

Other passages in the Bible also refer to this concept of honest weights. Leviticus 19:35-36 (*CSB*, 2017) says, “Do not be unfair in measurements of length, weight, or volume. You are to have honest balances, honest weights, an honest dry measure, and an honest liquid measure; I am the Lord your God, who brought you out of the land of Egypt.” Also, Ezekiel 45:10 (*CSB*, 2017) says, “You are to have honest scales, an honest dry measure, and an honest liquid measure.” There are also many other passages that address using honest weights, such as Amos 8:4-6, Hosea 12:7-8, Micah 6:10-14, Proverbs 20:10, Proverbs 16:11, and Proverbs 20:23 (*CSB,* 2017). Again, God is emphasizing that He wants businesses to be honest when they engage in trade. He does not want fraud to take place in the marketplace. This applies to dry products and can even apply to services that are provided. When a mechanic works on a vehicle, he should be honest with the amount of time that he spent to fix the vehicle. This is important because the customer will be billed based on the amount of time that is recorded by the company.

The same is true in accounting. If a company commits fraud, and as a result overstates their assets, understates their liabilities, and overstates their net income, they will appear more profitable than they really are to the public. This could lead to people investing in a company that they would otherwise not invest in if they had accurate information. In addition, a bank might lend money to the company based on the financial information they receive from the company. This type of deception has led to many large frauds such as Enron, WorldCom, and Arthur Anderson. Committing fraud has caused many employees to lose their jobs and has led to billions in losses for investors. Therefore, the accounting profession should always strive for ethics, or honest accounting, to provide financial statements to the public that accurately reflect the financial condition of the organization.

In summary, having a Biblical perspective when conducting research ultimately helps a researcher conduct better research. Implementing concepts such as integrity, objectivity, and trust helps research to make new discoveries that can benefit society. Companies benefit when their employees act in an ethical manner that mirrors biblical principles, and society ultimately benefits with better products and services when fraud is prevented in nonprofit organizations.

Relationship to Field of Study

Understanding the factors that contribute to fraud within nonprofit organizations was important to understanding how to prevent future frauds from occurring. By understanding these factors, steps can be implemented to reducing these issues which cause organizations to be at an increased risk of fraud. By identifying and addressing these factors, nonprofits can mitigate their risk of loss, and have resources available for their intended usage. Preventing more frauds from taking place will help to increase the trust of donors and other contributors that the resources of the organization are safe and secure. Better protected nonprofit organizations will benefit society with better operated charities, and better equipped employees to work at those organizations.

In addition, less resources will be wasted by fraudsters who misuse the organization’s resources, based on the one or more of the identified factors. This savings will benefit nonprofits as well as the people they serve, which will result in organizations being able to be better manage their resources. Therefore, better understanding the factors that lead to fraud can have a significant impact on both nonprofits and society.

Summary of the Significance of the Study

The significance of this study was to understand the internal control weaknesses in faith-based organizations. This study attempted to reduce the gaps in the existing literature by providing strategies that are specific to faith-based organizations. The research was closely associated with the field of study in accounting through the examination of fraud. This study also had implications for Biblical integration which can help reduce the risk of fraud within an organization.

A Review of the Professional and Academic Literature

A literature review was conducted on the strategies and internal control procedures that Nonprofit Organizations (NPO)s can implement to decrease the risk of fraud. There have been several studies conducted in this area of research both domestically and internationally. Several findings were uncovered from prior studies and research.

Overview of Nonprofit Frauds

Fraud is a major concern for both for-profit and nonprofit organizations. The nonprofit sector has become a major target of fraud since it has revenues of over $2.62 trillion per year, over $5.99 trillion in assets, and utilizes 65 million volunteers (NCCS, 2020). Nonprofits make up 5.4% of the United States GDP, which is equivalent to the sixteenth largest economy in the world (Applegate, 2019). The number of registered nonprofit organizations continues to grow and is now at 1.54 million, which is a 4.5% increase from the previous decade (NCCS, 2020). In addition, over 25% of adults in the United States volunteer at a nonprofit contributing an estimated 8.8 billion hours with a value of approximately $195 billion (NCCS, 2020). Nonprofits are involved in many areas of society including charitable, religious, education, health, scientific, human resources, and the economy (Ries, 2016).

Consequently, the Association of Certified Fraud Examiners (ACFE) stated in their *Report to the Nation* that nonprofits made up nine percent of all reported frauds and that their average loss was $639,000 (ACFE, 2020). The typical fraud transpired for 14 months before being detected and cost the organization $8,300 per month. Each year it is estimated that 5% of an organization's funds are lost by fraud (ACFE, 2020). This equates to approximately $40 billion in fraud losses each year (Greenlee et al., 2007). Asset misappropriation is estimated to represent over 95% of frauds committed in nonprofit organizations (Greenlee et al., 2007).

Some believe that nonprofit organizations are more susceptible to fraud because of their greater reliance on human decency, and lack of resources for implementing and monitoring internal controls (Abu Khadra & Delen, 2020). Many organizations have a strong influence of trust of their employees, even though many of them are volunteers, and may not have the experience of paid professionals (Soobaroyen & Sannassee, 2007). Even the board of directors at some nonprofit organizations are volunteers who may not have financial expertise (Greenlee et al., 2007). Those that should be establishing internal controls may have little or no training nor experience in that area (Greenlee et al., 2007). In one study, 64% of the frauds were committed by executive level employees (Archambeault & Webber, 2018). However, when a fraud is disclosed publicly, many donors may decrease support for that organization (Harris et al., 2017).

Numerous nonprofit frauds have made headlines causing donors and the public to question the trust that they have given these organizations. Frauds such as a $1.5 million employee theft at Memorial Sloan-Kettering Cancer Center, a $26 million scandal at New York University by an investment manager, and The Global Fund's $43 million worth of improper payments to grantees are just a few nonprofit frauds (Harris et al., 2017). Exorbitant executive spending by the Smithsonian Institution and Oral Roberts University, embezzlement of funds by

United Way, Angel Food Ministries, and Cancer Fund of America, and pyramid schemes by the Baptist Foundation of Arizona and New Era Philanthropy have broken the trust in nonprofits (Garven, 2015). In addition, the Federal Bureau of Investigation (FBI) reported that there were over 2,000 websites that were solicitating donations for Hurricane Katrina victims that were fraudulent (Greenlee et al., 2007). Every dollar that was stolen through fraud was money that was not used to provide a much-needed public service (Greenlee et al., 2007).

Frauds can occur in even large nonprofits that have the resources to implement internal controls. The American Cancer Society suffered a $7.5 million fraud by their chief administrative officer, Daniel Wiant, through several schemes he perpetrated including creating fictitious vendors, using employees' names to make charges with the organization's credit cards, making unauthorized bank transfers, and doctoring financial statements (Gallagher & Radcliffe, 2002). Fleming et al. (2016) found that larger organizations tend to have larger frauds, often involve multiple perpetrators, and are less likely to be discovered by accident. The American Cancer Society did have internal controls in place to prevent the fraud from taking place, such as two signatures for withdrawal of funds, an annual audit, and background check for new employees; however not all these controls were followed or monitored (Gallagher & Radcliffe, 2002). This fraud may have been viewed as a misnomer that could not have been prevented, however this was not the first fraud at the organization. The American Cancer Society had already suffered from fraud three other times, including an employee who embezzled $150,000 through stealing cash and writing checks to herself (Gallagher & Radcliffe, 2002). She was able to perpetrate the fraud because she had sole responsibility to one of the accounts in the organization (Gallagher & Radcliffe, 2002). In the case with Wiant who stole $7.5 million, the organization was able to recover the funds by putting a freeze on the bank account where he had transferred the money to (Gallagher & Radcliffe, 2002). The authorities were able to stop the fraud quickly in large part because of the arrogance of the perpetrator. Wiant had called his wife to tell her that he was leaving her and had stolen millions of dollars. His wife then went to the authorities, who were then able to act quickly. Wiant was sentenced to 13 and a half years in prison and ordered to pay a $500,000 fine (Gallagher & Radcliffe, 2002).

NPO Studies. Several studies have been conducted on nonprofit fraud. Abu Khadra and Delen (2020) conducted a study of 428 nonprofit organizations and analyzed 21 different measures over a six-year period. They obtained this data from Internal Revenue Service Form 990 filings and then used logistic regression and decision tree induction algorithms to study fraud reporting and governance characteristics. They found that 214 organizations had reported a major fraud; they also found that governance is an important factor for deterring fraud (Abu Khadra & Delen, 2020).

Another study was conducted by Archambeault and Webber (2018) to understand the survivial rates of nonprofit organizations that experienced a fraud. A scandal can lead to the complete demise of an organization, so they studied 115 organizations and discovered that over one fourth of these organizations did not survive after three years of a fraud being made public (Archambeault & Webber, 2018). They also learned that older and larger organizations are more likely to survive a fraud than smaller and younger ones; the average age of surviving organizations was 25.2 years compares to those that did not survive was 12.7 years (Archambeault & Webber, 2018). These organizations suffered from what they referred to as a liability of newness and liability of smallness. A liability of newness is where new organizations are more likely to fail than older ones due to a lack of experience and skills by employees, a lack of structure and routines, and a lack of relationships with external constituencies (Archambeault

& Webber, 2018). The liability of smallness states that smaller organizations are less able to withstand a fraud than a larger one due to their difficulty in raising capital, competition for labor, tax laws, and other regulations (Aldrich & Auster, 1986). Furthermore, frauds that involved executive-level personnel or where the organization vicitmized the public where less likely to survive (Archambeault & Webber, 2018). Lower level employees typically had less access to make significant transactions to commit larger frauds compared to executives, who had a broader access to the organization's assets and systems (Archambeault & Webber, 2018). Additionally, Kramer (2015) noted that the greatest percentage of fraud cases took place in organizations with less than 100 employees. Moore (2018) discovered that smaller organizations are disproportionately more affected by occupational fraud than larger organizations. As a result, small organizations are more at risk to fraud than larger ones.

A study was also conducted by Harris et al. (2017) to see if having strong governance would reduce the likelihood of fraud in a nonprofit organization. The study analyzed 764 charities: the results of the study indicated that keeping managerial duties in-house, conducting audits, and monitoring by debt holders are strongly associated with lowering the rate of fraud (Harris et al., 2017). Although the job of an external auditor is not primarily to detect fraud, conducting an external audit is negatively associated with the risk of asset diversions, which means that external audits deter and detect frauds (Harris et al., 2017). The same is true when the board of directors review the organization's Form 990; there is a negative association between the review and the risk of fraud (Harris et al., 2017). This form of monitoring helps the organization mitigate their risk of asset diversions. Therefore, the study suggests that stronger governance in nonprofits may reduce the risk of fraud within these organizations. Halbouni et al.

(2016) found similar results on the effect of corporate governance in preventing and detecting fraud.

Snyder et al. (2017) conducted a study on frauds committed against 501(c)(3) nonprofit organizations. Data were provided by GuideStar, which is an information services company that specializes in nonprofit data for the United States (Snyder et al., 2017). They received surveys from 1,396 responses and found that 19% of the organizations experienced some type of fraud within the last five years (Snyder et al., 2017). They also discovered that there are two control practices that are performed less frequently by those organizations that have experienced fraud than by those who have not. Those practices are the review of expenses by the board of directors and the enforcement of the organization's vacation policies (Snyder et al., 2017). In addition, they found that organizations that did experience fraud made several changes to their internal controls afterwards. These changes included reference checks, job rotation, board review of expenses, vacation policy enforcement, board training in financial management, bonding of employees, and physical security review (Snyder et al., 2017). In addition, these organizations decreased their practice of spending more than budgeted and avoided pre-signing checks (Snyder et al., 2017). Several simple internal controls were recommended that all organizations can benefit from. They stated that all nonprofits can become a victim of fraud, and that some charities think that their charitable mission will insulate them from embezzlement or asset misappropriation (Snyder et al., 2017). Snyder et al. (2017) also suggested that organizations pay attention to what is happening in their organization since most frauds are simple and easy to detect. They also recommended that the duties surrounding collecting and spending money should be divided among several employees (Snyder et al., 2017). For example, having more than one employee count money, examining bank statements, and having an employee other than the treasurer make bank deposits are just a few ways to segregate duties (Snyder et al., 2017).

Fraud has also been studied in charities located in England. Ohalehi (2019) interviewed 20 randomly selected small charities (annual income under £250,000) to better understand the challenges they faced regarding fraud. He found that small charities suffered losses due to weak internal controls systems, a lack of segregation of duties, and poor governance (Ohalehi, 2019). This is due in part to the limited resources of smaller charities and their greater reliance on volunteers and trustee daily management (Ohalehi, 2019). The study also revealed that 92% of the interviewees have some type of system in place to detect and prevent fraud in their organization, however, 63% admitted that they do not have a formal policy in place for dealing with financial crime cases (Ohalehi, 2019). Twenty-two percent stated that they would report fraud cases to the auditors, and four percent stated that they would conduct a forensic audit (Ohalehi, 2019). Consequently, small charities should have systems in place to protect against fraud because small charities that do suffer from fraud do not always have the resources to survive a fraud (Ohalehi, 2019).

Greenlee et al. (2007) studied 58 nonprofit organizations where fraud had been committed. These cases of fraud ranged from $200 to $17 million with a median loss of $100,000 (Greenlee et al., 2007). From these cases 25% of the frauds were committed by managers, and 8.6% were perpetrated by executives (Greenlee et al., 2007). They found that larger fraud was associated with collusion, higher salaries, age, educational level, and longer tenure with the organization (Greenlee et al., 2007). The median size frauds however had different characteristics. These frauds resulted in losses of less than $50,000, involved women with no prior criminal record who had worked at the organization for at least 3 years. The median age of the perpetrators studied was 41, and the median tenure at the organization was 7 years (Greenlee et al., 2007). Collusion also was a major factor in the size of the fraud. The median loss from frauds that involved collusion were four times higher than those committed by individuals (Greenlee et al., 2007). Ninety-seven percent of the reported frauds were asset misappropriations and 95% of the misappropriations involved cash with a median loss of $100,000 (Greenlee et al., 2007). Out of the cash misappropriation frauds 75% of the cases involved fraudulent disbursements (Greenlee et al., 2007). Therefore, fraudulent disbursements, which is paying for an expense that the company does not owe, was the most common form of fraud from this study. The least common type of fraud was financial statement fraud (5% of the sample), however, the median loss ($3 million) was 30 times greater than the other frauds (Greenlee et al., 2007).

In this study 72% of the cases led to the termination of the employees involved, and 7% resulted in no punishment for the perpetrator (Greenlee et al., 2007). Those who were not punished often quit or disappeared before they could be punished. Those who had committed large frauds were criminally prosecuted in 72% of the cases (Greenlee et al., 2007). Of those that were accused, 70% pled guilty and 25% the prosecutor declined to prosecute for reasons such as lack of sufficient evidence (Greenlee et al., 2007). Oftentimes perpetrators were not prosecuted to protect the reputation of the organization. However, prosecution would have helped the perpetrator experience consequences and perhaps help them to stop committing fraud (Gray & Villamarin, 2015). In addition, some insurance policies require prosecution of a case to collect coverage from fraud. Furthermore, failure to prosecute may prevent future employers from unknowingly hiring an employee that has committed fraud (Gray & Villamarin, 2015).

Tremblay-Boire and Prakash (2015) conducted a study to better understand online disclosures made by nonprofits in the United States. Their research included analyzing 201 American nonprofits from the Chronicle of Philanthropy's Philanthropy 400 (Tremblay-Boire & Prakash, 2015). The data were obtained from the IRS Form 990 filings over a 3-year period; churches, church-affiliates, and public universities were excluded from the study since they are not required to file a Form 990 (Tremblay-Boire & Prakash, 2015). From their study they found that large nonprofits, religion-related nonprofits, and health sector nonprofits disclose less information to the public (Tremblay-Boire & Prakash, 2015). Conversely education nonprofits tended to disclose more accountability information to the public (Tremblay-Boire & Prakash, 2015). Nonprofits in general tended to provide accountability to the public with the desire to safeguard and enhance their reputation (Tremblay-Boire & Prakash, 2015).

Another study involved 22 participants in nonprofit organizations in the state of Delaware. This study found that the greatest challenges are transparency, controls over expenditures, and that smaller nonprofits struggle with controls because of a lack of resources (Baapogmah et al., 2015). Smaller organizations also struggled with internal controls because they typically consisted of long-term friends and family (Bunn et al., 2019). These organizations relied on trust, love, and a culture of family (Bunn et al., 2019).

A study was conducted in Canada to better understand nonprofit frauds that were occurring within the country. The nonprofit and voluntary sector of Canada employs 12% of the population and accounts for 6.8% of the country's gross domestic product (GDP; Hall et al., 2005). The study found that senior management positions were the most frequent perpetrators of fraud in Canada, and that most perpetrators worked for the organization for more than 10 years, and were 30 to 50 years old (Chen et al., 2009). In addition, 42.86% of the frauds that were committed took place in a nonprofit that had ten or fewer employees (Chen et al., 2009). Almost all the frauds (96%) involved asset misappropriation (Chen et al., 2009). They also found that most of the frauds were committed by individuals instead of by collusion, and the most perpetrators had no prior criminal record (Chen et al., 2009). However, those who were charged and convicted did serve at least some jail time (Chen et al., 2009). Out of the frauds studied, 36% were detected by accident, 27% by internal audit, 18% by external audit, 5% by tip, and 14% by internal controls (Chen et al., 2009). Eighty-two percent (82%) of the frauds in the study were committed in metropolitan areas which contained 60% of the country's population, showing that a disproportionate number of frauds took place in larger cities (Chen et al., 2009).

Another study was conducted on 300 Non-Governmental Organizations (NGO)s in Mauritius (Soobaroyen & Sannassee, 2007). This study found that very little information about their accounting practices and internal controls is disclosed. Annual reports of nonprofits in Mauritius are not released to the public, and these organizations are not monitored by tax authorities (Soobaroyen & Sannassee, 2007). Similarly, in other countries nonprofit accounting data are often not released to the public. In the United Kingdom only twenty four percent of charities disclose budget-related information, and only three percent of small charities release such data (Connolly & Hyndman, 2004).

Soobaroyen and Sannassee (2007) found that these nonprofits had physically present internal controls, however they were not functionally present. Their control practices were not enforced, monitored, or used to deter fraud. Soobaroyen and Sannassee (2007) believed that these organizations implemented a symbolic use of internal controls to conform to some form of external rules or other cultural-cognitive motivations. Budgets were not always prepared, and if they were, they were rarely circulated and use by the organization (Soobaroyen & Sannassee, 2007). Approval of the annual reports were a formality, with most communication being conducted occasionally on an informal basis (Soobaroyen & Sannassee, 2007). Since adoption of financial practices is voluntary, few nonprofit organizations see the need to implement them, unless required by other outside regulations (Soobaroyen & Sannassee, 2007).

A study was also conducted in Malaysia to better understand internal controls and supervision mechanisms in nonprofit organizations located in developing countries (Othman & Ali, 2014). In Malaysia proper accounting standards are not always available, and with laws not being enforced, many nonprofits do not prepare financial statements; consequently, disclosure of financial information is very low by nonprofits in Malaysia (Othman & Ali, 2014).

Othman and Ali (2014) surveyed 60 charities about their internal controls and found that effective supervision and better internal controls can help promote transparency and accountability, which will attract more donors. Their survey results showed that only 12% of the charities had the minimum recommended internal control practices in place (Othman & Ali, 2014). Nonprofits limited resources were one factor for a lack of internal controls; one third of nonprofits in Malaysia had income of less than $650 per month (Othman & Ali, 2014). Another factor for poor internal control practices was that the controls are not mandatory, and there are no best practices available (Othman & Ali, 2014). Having low internal controls can increase the risk of fraud. To compensate for a lack of controls Othman and Ali (2014) recommended analyzing annual reports that have significantly higher than usual administrative costs. They also believe that the government should subsidize the cost of accounting services for nonprofits, provide training for charities, and guidelines for nonprofit accounting practices (Othman & Ali, 2014). Standard rates for meals, travel, and lodging would also help to limit fraud, as well as requiring independent auditors, and subsidizing the cost of audits (Othman & Ali, 2014). They recommended that government oversight should be efficient and limited, to include monitoring organizations to ensure they submit their required annual financial statements (Othman & Ali, 2014).

The Association of Certified Fraud Examiners conducted a study on fraud in nonprofits to determine the frequency of each type of fraud that is committed. In their *Report to the Nations* they summarized the percentage of cases that are related to each type of scheme (ACFE, 2020). Table 1 depicts the summary of their findings.

Table 1

Nonprofit Schemes by Percentage

Nonprofit Schemes	Percent of cases
Corruption	41%
Billing	30%
Expense reimbursement	23%
Cash on hand	17%
Noncash	16%
Skimming	15%
Check and payment tampering	14%
Cash larceny	12%
Payroll	12%
Financial statement fraud	11%
Register disbursements	3%

Notes. Percentages do not add up to 100% since some frauds involved more than one scheme. Compiled from data from ACFE (2020).

Faith-Based Organizations. Faith-Based Organizations (FBO)s are a subset of Non-Profit Organizations (NPO)s in that the employees, volunteers, and donors of the organization generally share a common faith or religious affiliation. Most faith-based organizations are charities. A nonprofit organization is one that seeks to provide a good or service to society without seeking a financial profit. A charity is a subset of nonprofits; charities are organizations that have received tax exempt status from the IRS and are sometimes referred to as 501(c)(3) organizations (Garven, 2015). A newly formed nonprofit organization must apply for charity status through the IRS; otherwise donations are not tax deductible for donors. Those charities (except churches and a few others) that do have tax exempt status must file a tax return called a Form 990 each year (IRS, 2020).

Christians give over $850 billion to causes each year, which includes $309 billion to churches, $464 billion to para-church agencies, and $44 billion to global foreign missions (Johnson et al., 2015). Faith-based organizations suffer from some of the same internal control weaknesses experienced by other nonprofits. Johnson et al. (2015) estimated that $50 billion of money given by Christians will likely be stolen from churches, para-church organizations, and secular organizations globally each year.

Faith-based organizations are susceptible to affinity fraud, which is fraud that exploits the trust of others, because people believe that other members share similar values that they have (Johnson et al., 2015). Therefore, faith-based organization are more likely to trust employees and volunteers instead of relying on internal controls. In addition, Applegate (2019) reported that 53% of all churches in the United States had not had a complete audit conducted in the previous year.

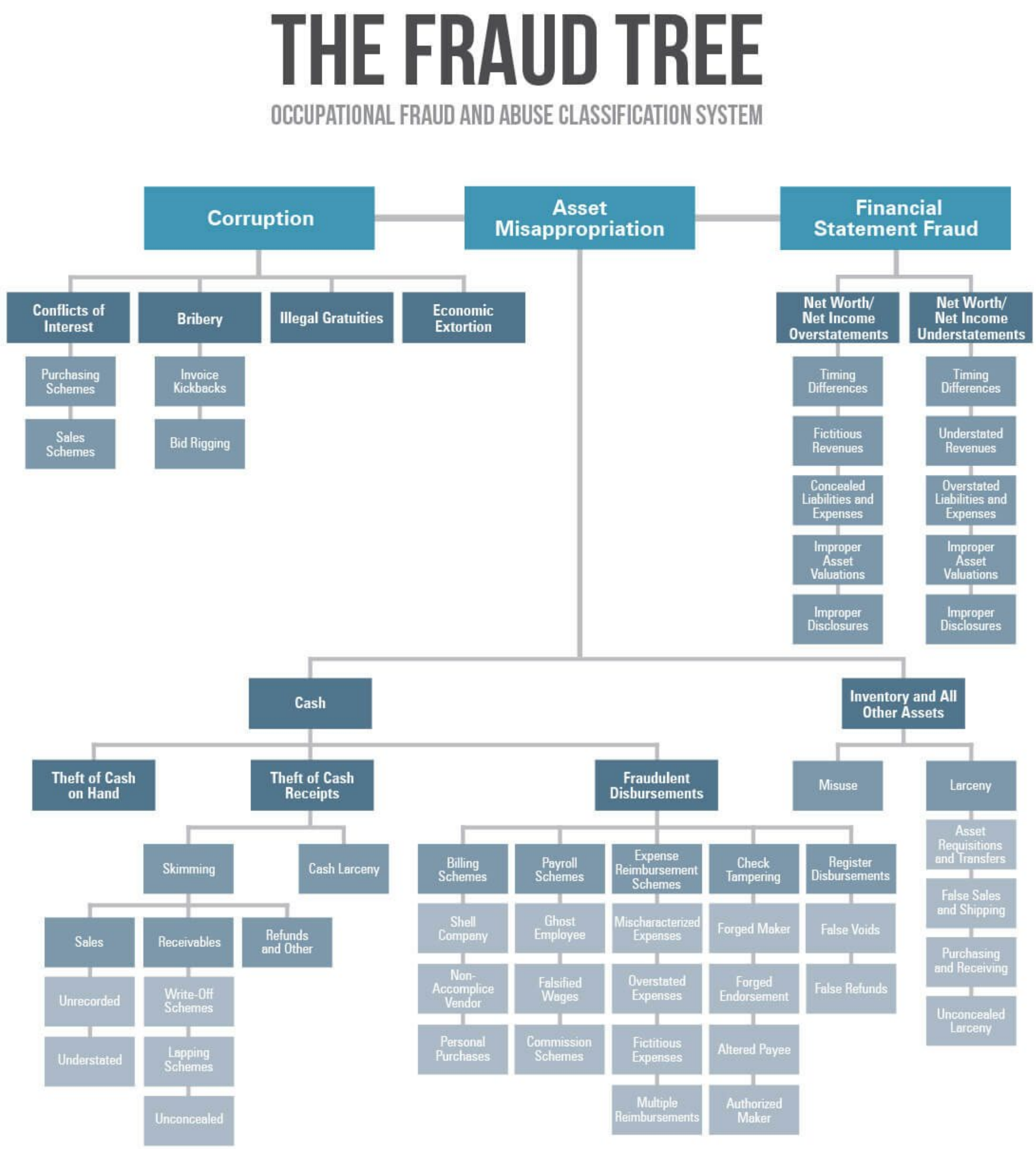
Fraud Theories

There are several theories regarding fraud and why and how it occurs. Fraud is defined as the intentional practice of deceiving, misrepresenting the truth for the purpose of causing injury or depriving another of their right (“Fraud,” 2020). Fraud must be intentional, otherwise it may fall under the category of negligence, which could occur if an employee makes a mistake or error from being careless. Wells (2014) wrote a textbook on fraud examination, and states that four elements must exist for fraud to be present. A statement must be materially false and knowledge that the statement is false; a victim relies on the statement, and suffers damages as a result (Wells, 2014).

Others have classified frauds into various categories. Harris et al. (2017) categorized fraud as asset misappropriation, financial statement falsification, or corruption. The ACFE (2020) defined occupational fraud as a type of fraud where employees, officers, or directors attack an organization from within. Wells (2014) categorizes frauds as either against the organization itself (such as misappropriation of cash), or against the stakeholders of the organization (such as falsifying the financial statements). The ACFE has further categorized occupational frauds into three categories as seen in Figure 2 (ACFE, 2020).

Figure 2

Occupational Fraud and Abuse Classification System



Source: ACFE (2020). Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

Corruption is the first category, which is the wrongful use of influence to obtain benefits for one's self at the expense of the employer (Greenlee et al., 2007). Corruption is the most common type of scheme in every region of the world (ACFE, 2020). There are four major types of corruption which are bribes, rewards, extortion, and conflicts of interest (ACFE, 2020). Jeong and Siegel (2018) found that companies that have had a long-term high social status but are facing mediocre economics performance are at increased risk of large-scale corporate bribery. Rewards are improper gifts that are paid or received after the fraud; extortion are assets obtained by force of threat of force (Greenlee et al., 2007).

Asset misappropriation is the second category of occupational fraud. The median loss from this category of fraud is $100,000 per case (ACFE, 2020). There are three major types of cash misappropriations, which are theft of cash on hand, theft of cash receipts, and fraudulent disbursements. Theft of cash receipts includes skimming and cash larceny. Skimming is when cash is stolen before it is recorded, larceny is when cash is stolen after it is recorded, and fraudulent disbursements is when an organization pays for an expense that is not owed (Greenlee et al., 2007). Skimming could occur when an employee accepts money from an outside party, and instead of recording the sale pockets the money (Marks & Ugo, 2020). Larceny can occur when an employee takes cash or checks before they are deposited in the bank (Marks & Ugo, 2020).

The fraudulent disbursements category includes five types of frauds, which are billing schemes, payroll schemes, expense reimbursement schemes, check tampering, and register disbursements. Billing schemes are the most popular disbursement fraud according to one study (50% of fraudulent disbursements cases), and register disbursements fraud was the costliest, with a median loss of $350,000 (Greenlee et al., 2007). A billing scheme is where an employee submits a fraudulent invoice to the organization for payment that they are not entitled to receive (Marks & Ugo, 2020). This type of scheme generally involves setting up shell companies and billing for goods or services that were not received or excessively marking up the invoice amount to divert the excess to the fraudster (Marks & Ugo, 2020). Employees may also try to steal from an organization by overpaying a legitimate vendor and then stealing the overpayment when it is returned to the organization (Marks & Ugo, 2020). Additionally, an employee may purchase merchandise that is for personal use by inappropriately using the organization's funds (Marks & Ugo, 2020).

Financial statement fraud is the third category of fraud. This occurs when the organization overstates revenues, understates expenses or liabilities, reports assets at more or less than their actual value, recognize revenue or expenses in the wrong period, or fails to disclose significant information (Greenlee et al., 2007). Financial statement fraud is the least common category of frauds (10%), however when it does occur it is the costliest to the organization per case ($954,000 median loss; ACFE, 2020). Regarding financial statement fraud, it is believed expense misreporting is the most prevalent type of fraud (Greenlee et al., 2007). This occurs through the manipulation of the program expense ratio, which is a key ratio that donors review when determining how efficient an organization is operated.

The ACFE (2020) found that the nonprofit sector was at greater risk for corruption (41% of cases) billing schemes (30% of cases) and expense reimbursement fraud (23% of cases). Greenlee et al. (2007) reported that most frauds are committed by individuals with no prior criminal record. Men commit 72% of occupational frauds and cause a median loss of $150,000 whereas women cause a median loss of $85,000 (ACFE, 2020). The position that an employee has in the organization also affects the size of the average fraud loss. The median lower level employee fraud at a nonprofit is $21,000 per case, whereas frauds committed by managers had a median loss of $95,000 (ACFE, 2020). For frauds committed by executives or owners at nonprofits the median loss was $250,000 (ACFE, 2020). Lower level employees committed fraud in 23% of the cases, managers were involved in fraud in 35% of the cases, and executives or owners were the perpetrator of fraud 39% of the time (ACFE, 2020). More than half of all occupational fraud occurs in one of four departments: operations, accounting, upper management, or sales (ACFE, 2020).

In addition to fraud that originated from within the organization, there are also frauds that can occur from outside of the organization. These types of frauds can be attempts to commit fraud against an organization or against individuals. Attacks against an organization include vishing, which involves contacting employees via telephone for information, or phishing, which is an attempt for information via e-mail (Galletta, 2015). Vendor fraud is when a supplier overcharges, bribes, sells inferior goods, price fixes, creates shell companies, or offers potential kickbacks (Galletta, 2015). Organizations can also be susceptible to pharming, where a hacker redirects website traffic to a phony website with even a similar web address (Galletta, 2015). Frauds by individuals against other individuals would include frauds such as Ponzi schemes, where an investment opportunity is just initial investors being paid money raised from later investors (Galletta, 2015).

Fraud Triangle. The fraud triangle developed by Cressey (1950) was discussed earlier in the conceptual framework section, which includes three elements of fraud, which are pressure, rationalization, and opportunity (Kelly, 2017). Several others have built upon the theoretical groundwork of the fraud triangle. Harrison et al. (2018) described a dark triad, which are three personality traits that can be a predisposition that can lead to fraud behavior and intentions.

These three traits are narcissism, Machiavellianism, and psychopathy (Harrison et al., 2018). Narcissism is when someone has a strong need for admiration and attention, an inflated sense of their own importance, and a lack of empathy for others (Mayo Clinic, 2020). This trait allows a person to act unethically because it will be of personal benefit, and it alters their perception of their ability to successfully commit the fraud (Harris et al., 2017). Machiavellianism is a trait that has indifference to morality, includes callousness, and focuses on manipulativeness (Jones & Paulhus, 2009), and psychopathy is characterized by persistent antisocial behavior, impaired remorse and empathy, and disinhibited egotistical traits (Hare, 1999). Machiavellianism alters one's perception regarding the opportunities to commit fraud, and psychopathy affects how one rationalizes fraudulent behavior (Harris et al., 2017). This theory is an attempt to understand why and how some individuals choose to act unethically, and what personality traits influence fraud and the decision-making process (Harris et al., 2017).

The character traits of the dark triad influence the elements of the fraud triangle. In a study by Harris et al. (2017) psychopathy has a significant and substantive effect on rationalization, the trait Machiavellianism effects the opportunity and motivation elements of the fraud triangle. Rijsenbilt and Commandeur (2017) studied all Standard and Poor (S&P) 500 CEOs with more than three years of tenure and found that narcissism is a potential cause of fraud. CEOs also pose a risk to fraud due to their unique position. They are a risk due to the power they have in their position, heavy board expectations, the CEO aspirations for positive results, and the compensation structure of CEOs (Schnatterly et al., 2018). Harris et al. (2017) believed that individuals who have the predispositions of the dark triad traits and the elements of the fraud triangle will move to the moral stage of intention, and eventually to the action of committing fraud.

Another addition to the fraud triangle is the crime triangle. This triangle shows that crimes occur when three events occur: a motivated perpetrator finds a target at a specific place and time in the absence of a guardian (Mui & Mailley, 2015). Mui and Mailley (2015) believed that both the fraud and crime triangles should be used to provide a comprehensive view of a fraud event.

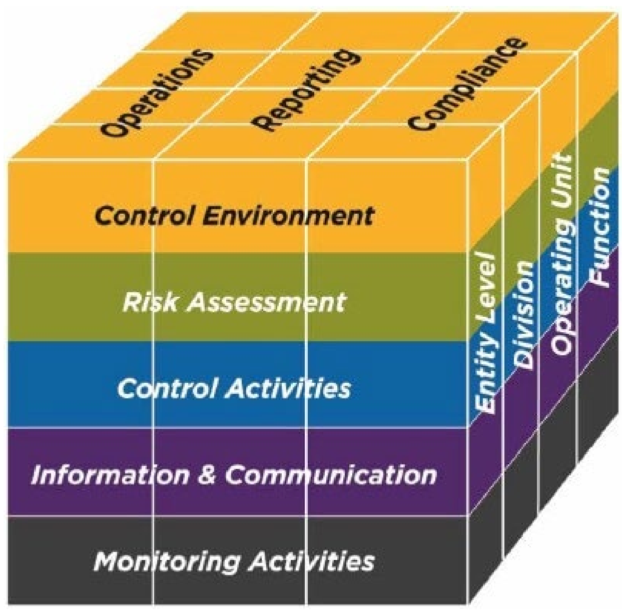
The fraud triangle is not without its critics. Some have argued that the fraud triangle is not an accurate theory to describe fraud. Murphy and Free (2016) found that fraud has a social dimension which is not addressed by the fraud triangle. Murphy and Free's (2016) study showed that 39% of respondents believe that instrumental climate was present when fraud was committed at their organization. Others state that all three elements of the fraud triangle do not need to be present for fraud to occur, and that the theory does not address fraudsters that are highly organized (Lokanan, 2015). Huber (2017) believed the fraud triangle is better labeled the embezzlement triangle because it only describes the theft of assets. He believes that fraud is based on misstatement, intent, reliance, material fact, and damage or injury more than it is about opportunity, motivation, and rationalization (Huber, 2017). Furthermore, Huber (2017) believed that there are many additional factors that contribute to the occurrence of fraud including personal, organizational, regulatory, economic, political, cultural, and sociological factors.

Fraud Diamond. Wolfe and Hermanson (2004) found that there is another element to the fraud triangle that was not included in the original theory. This fourth element is capability, and states that an individual's abilities and traits are major factors in the perpetration of fraud (Abu Khadra & Delen, 2020). Capability can come in the form of the perpetrator's position in the company, their intelligence in understanding how to exploit the internal controls, the ego and confidence that they will not be detected, and the capability of dealing with the stress of being caught (Ruankaew, 2016). This additional element has led to the fraud triangle to become known as the fraud diamond (Albrecht et al., 2016). Some studies have suggested that this framework better identifies fraud risks (Boyle et al., 2015). Others have added additional elements, such as Sorunke (2016), who suggest a fraud pentagon by adding personal ethics as a missing trait.

COSO Framework. Another framework for this study was the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework. This framework was developed in 1992 and has been used by auditors and accountants globally to address the risk of fraud, and the means to mitigate that risk. This framework is made up of five components, which are the control environment, risk assessment, control activities, information and communication, and monitoring activities (COSO, 2017). This framework is depicted as a cube as shown in Figure 3.

Figure 3

COSO Framework



Source: COSO (2017).

The control environment is the organization's commitment to ethical values and integrity (COSO, 2017). Having a high level of integrity will reduce the risk of asset misappropriation (Bakri et al., 2017). Risk assessment is when the organization considers the potential fraud risks (COSO, 2017). Once an organization has identified the potential risks, management will respond to each risk with one of the four options: avoiding, reducing, sharing, or accepting (Applegate, 2019). Risk assessment can involve both internal and external risks (Ries, 2016). Internal risks include risks surrounding programs, administration, personnel, and support; external risks involve risk related to vendors, contractors, donors, and regulators (Ries, 2016). Control activities are policies and procedures that contribute to the mitigation of risk; information and communication is when the organization uses relevant information to communicate internal controls to both internal and external parties; monitoring activities is the ongoing evaluation that internal controls are present and functioning (COSO, 2017). Monitoring is an important element of the framework to ensure that internal controls are implemented, relevant, and being complied (Rae et al., 2017). Based on a study conducted by Abdul Rahman and Al-Dhaimesh (2018), they believe that all employees can assist with identifying fraud risks. The COSO framework has also been used to create fraud risk management principles with the primary goal of mitigating the risk of fraud (COSO, 2016).

In addition to the five components of the COSO framework, there are three objectives, which are represented as columns on the COSO cube. These three objectives are operations, reporting, and compliance (COSO, 2017). Operations objectives refers to the efficiency and effectiveness of an entity's operations, which includes safeguarding assets from loss and meeting financial performance goals (COSO, 2020). Reporting objectives includes terms such as reliability, transparency, and timeliness as determined the organization's policies, regulators, and other standard setters (COSO, 2020). Compliance objectives refers to adherence to regulations and other laws that the organization is subject to (COSO, 2020).

The third side of the COSO cube is the organization's structure. The organization's structure can be viewed from several different perspectives. These perspectives include the entity level, division level, operating level, and functional level (COSO, 2020).

Several studies have been conducted to analyze this framework. Le and Tran (2018) studied the five components of the framework through questionnaires collected from accountants, internal auditors, and managers in Vietnamese organizations. The data collected showed that the control environment are believed to have the strongest impact on reducing the risk of fraud followed by control activities and information and communication8 components (Le & Tran, 2018).

The COSO framework includes components, objectives, and organizational structure. These three sides of the COSO framework are related to each other. Each of the framework's components can be analyzed by objective; for example, the control environment component can be used to analyze the organization's operations, reporting, or compliance separately. In addition, the organizational structure perspective is related to the components and objectives. For example, internal controls can be reviewed for an individual department or for the entity as a whole. In addition, the reporting objective can be applied to smaller segments within the organization or to the entire organization. Therefore, the components, objectives, and organizational perspective are related to each other as depicted by the COSO cube.

Other Factors. There are several other factors that may lead to fraud within an organization. Some of those factors may include an organization's ethical culture, market pressures, structures that limit oversight, and unreasonable performance goals (Archambeault &

Webber, 2018). Others have cited that weak internal controls, an atmosphere of trust, lack of financial expertise, and reliance on volunteer board members as contributory factors to fraud (Douglas & Mills, 2000). This reliance on trust has allowed some nonprofit organizations to overspend on administrative expenses due to weaker monitoring and governance in the nonprofit sector (Felix et al., 2016). Personal characteristics that can be a red flag that employees might commit fraud is when they have high personal debts and are living beyond their means (Greenlee et al., 2007). Organizational characteristics that can also contribute to fraud is when the organization does not have clear lines of authority, procedures for authorization of transactions, and lax enforcement of policies and procedures (Greenlee et al., 2007). Murphy (2015) found that common fraud issues in nonprofits include stolen donations, misclassified restricted donations, related party transactions, improper expense reporting and reimbursement, management override of controls, and lack of segregation of duties. He also noted that unreasonable budget expectations can put pressure on employees to create fraudulent financial statements (Murphy, 2015).

Organizations may also suffer from fraud through collusion. Collusion is when two or more employees work together to commit fraud. This type of fraud is more difficult to detect because the employees may be able to circumvent an internal control by working together. Free and Murphy (2015) identified three types of bonds that are formed while committing collusion. The first type is individualistic, where two or more employees work together to provide individual benefits (Free & Murphy, 2015). This could be two employees working together to steal cash, where each is stealing cash for their own benefit. The second type of collusion is collectivistic, which involves multiple employees working together for organizational benefits. An example would be manipulating the financial statements so that the organization appears more profitable. The third type of collusion is relational, which is based on positive regard for another (Free & Murphy, 2015). This could be an employee not reporting a fraud because the perpetrator was a family member or close friend.

In addition to fraud organizations can make errors in their accounting systems. Burks (2015) found that nonprofit organizations make 60% more errors than their publicly traded counterparts. The most common errors that public charities make are errors of omission, where the organization fails to record a transaction (Burks, 2015).

Fraud Prevention and Mitigation

One of the financial goals of nonprofits is to prevent and detect fraud. Fraud can be prevented or mitigated using internal controls and other fraud prevention strategies. These tools can help management reduce the risk of fraud by reducing the opportunity for fraud to be committed. One way to combat against the fraud triangle is with the antifraud triangle. The antifraud triangle is composed of three components, which are prevention, detection, and insurance (Pedneault, 2010). Another version of the antifraud triangle is values, culture, and controls (Kelly, 2017).

Reporting Fraud. PricewaterhouseCoopers (PwC) discovered that on average organizations experienced six incidents of fraud, and that nearly half of all organizations have experienced at least one fraud over the last two years (PwC, 2020). However, oftentimes fraud does not get reported by nonprofit organizations for fear of loss of trust by donors and other entities that may contribute to the organization (Boenigk & Becker, 2016; Jeavons, 2001). In 2008, the IRS began requiring that nonprofits disclose significant frauds on their Form 990 tax return (Abu Khadra & Delen, 2020). Reporting frauds, or significant asset diversions as named by the IRS, includes any unauthorized conversion or use of the organization’s assets other than for the organization's authorized purposes, including, but not limited to, embezzlement or theft (IRS, 2020). A significant diversion of assets is defined by the IRS as one that exceeds the lessor of: five percent of the organization's gross receipts for the tax year; five percent of the organization's total assets as of the end of its tax year; or $250,000 (Abu Khadra & Delen, 2020). Even though the IRS began requiring that organization report fraud on the tax return, not all organizations have self-reported. Archambeault et al. (2015) found that 33% of the organizations in their study did not disclose a fraud even though they should have made the disclosure. In addition, only half of the frauds were reported to law enforcement out of those where confession of wrongdoing was admitted (Bonny et al., 2015).

Internal Controls. The use of internal controls is an effective method that organizations can use to reduce the risk of fraud (Dimitrijevic et al., 2017; Zakaria et al., 2016). The ACFE (2020) found that lack of internal controls contributed to one third of frauds. Greenlee et al. (2007) found that 14% of frauds are detected using internal controls. Since nonprofit organizations have fewer internal controls in place, they are more vulnerable to fraud (ACFE, 2020). The top three control weaknesses in nonprofits are lack of internal controls (35% of organizations), lack of management review (19%), and ability to override existing internal controls (14%; ACFE, 2020). Nonprofits are also less likely to have surprise audits, formal risk assessments, management review, and an internal audit department than for-profit companies (ACFE, 2020). Internal controls can also increase the efficiency of management by putting in systems that reduce the need to micromanage all employees' actions (Kazantseva & Plotnikov, 2018). Internal controls are designed to reduce the risk of fraud. Internal controls can be either detective or preventative. Detective controls should be designed to detect fraud quickly so that it is unable to continue for long periods of time (Simha & Satyanarayan, 2016). No set of controls and strategies can guarantee that fraud will be prevented. If employees are colluding together, if management is overriding controls, or if mistakes are being made, there will be a risk of fraud (Dickens & Fay, 2017).

Audit Committee. An audit committee is an important group that helps to reduce the risk of fraud within an organization. This committee should oversee the audit of the organization but can also provide oversight of management's performance (Greenlee et al., 2007). The committee typically contains three to five members with at least one member that is a financial expert (Marks & Ugo, 2020). The members that serve on the audit committee should be independent board members (Greenlee et al., 2007), and independent from management (Marks & Ugo, 2020). They should also have the authority to hire outside counsel and advisors as needed (Marks & Ugo, 2020).

Conflict of Interest Policy. The opportunity for fraud to occur increases when there is a conflict of interest within an organization. A conflict of interest policy is a type of control that can help mitigate this risk. Most corruption cases occur because of a conflict of interest in the organization (Todd, 2016). Harris et al. (2017) found that organizations that have a conflict of interest policy have a lower risk of asset diversion because it improves decision-making and transparency. Key employees, officers, and directors that have business relationships or family connections with the organization should disclose those relationships (Abu Khadra & Delen, 2020). Failure to do so could increase the risk of asset misappropriation. Creating a policy against conflicts of interests and enforcing such policies will help to reduce the risk of fraud.

Whistle Blower Policy. Another internal control that organizations should have is a whistle blower policy (Kummer et al., 2015). This policy provides a means for individuals to report suspicions of fraud anonymously. Whistleblower tips are the most effective fraud detection method, with 40% of occupational fraud in nonprofits being detected through this method (ACFE, 2020). Half of these tips are from employees within the organization, so providing a means for reporting suspicion of fraud is important (ACFE, 2020). This can take the form of a tip hotline where employees can call or submit in writing anonymously when fraud is suspected. Tips have been used to uncover nearly three times as many frauds as other forms of detection such as audits, management monitoring, and surveillance devices (Marks & Ugo, 2020). The Internal Revenue Service stated that since the Dodd-Frank Act of 2010 whistleblowing has become more desirable and has experienced a 322% increase in 2016 (Latan et al., 2019). There are four factors that influence whether someone will whistle blow concerning a fraud; the factors are pressure, financial incentives, rationalization, and opportunity (Latan et al., 2019). Latan et al. (2019) found that financial incentives are the most significant influence of an auditor's intention to whistle blow. Johansson and Carey (2016) also found that anonymous reporting channels are an effective tool to detect fraud against organizations. In addition, smaller organizations can receive the greatest benefit from implementing an anonymous reporting channel (Johansson & Carey, 2016). Hess and Cottrell (2016) found that third party hotlines are available for smaller organizations that provide 24-hour anonymous phone and email support in multiple languages for as little as $500 per year. Peltier-Rivest (2018) found that only 74% of organizations offered the ability to report a tip anonymously. More organizations should provide anonymous protection, and all credible allegations should be investigated (Peltier-Rivest, 2018).

Free (2015) stated that some organizations have provided employees with anti-retaliation protections, and incentivized reporting with monetary rewards. Some have even imposed liabilities for failure to report a suspected fraud (Free, 2015). Laws have been passed to prevent retaliation on whistleblowers for publicly traded corporations (Murphy, 2015). These types of policies can also be implemented for nonprofits to protect whistleblowers.

External Audit. Another control that can help deter fraud is to hire external auditors to conduct an audit. Since 60% of frauds are perpetrated by executive management, it is important that there is oversight using an audit committee, which can oversee the annual audit (Greenlee et al., 2007). Paying for an audit provides more than the service of the external auditors. There is also the perception factor. Employees are less likely to perpetrate a fraud if they know that the financials will be audited each year. The perception that the auditors will review documentation is enough to deter some employees from committing fraud. Most of the nonprofit organizations studied by Abu Khadra and Delen (2020) hired external auditors to conduct an audit and made use of an audit committee. Greenlee et al. (2007) found that 12% of frauds are detected by the external auditors. Therefore, this can be an effective control to deter fraud within an organization. Auditors with experience in information technology (IT) internal controls can also be beneficial (Haislip et al., 2016). Garven et al. (2018) found that nonprofits do not have to hire one of the Big 4 accounting firms to get a high-quality audit performed; many medium size audit firms are able to provide high-quality financial audits. Although an external audit may discover a fraud, an organization cannot assume that if there is a fraud the auditors will catch it (Marks & Ugo, 2020). The primary responsibility for discovering fraud is with the management or board of directors of the organization. Even if the external auditor can discover a fraud, it is oftentimes too late to prevent the reputational and financial damages that will occur (Marks & Ugo, 2020). Reputational risk can be one of the greatest risks that a nonprofit organization faces (Ries, 2016). Some nonprofit organizations are required to undergo an annual audit (those that have spent more than $750,000 in federal monies in a year), but for those who are not, an external audit is still a beneficial control for organizations (Park et al., 2017).

Internal Audit. In addition to an annual external audit, an internal audit department can help an organization detect and prevent fraud (Aris et al., 2015). The ACFE (2020) found that 17% of frauds in nonprofits are discovered by the internal audit department. Organizations that are large enough to be able to have internal auditors can benefit from their efforts. Ege (2015) found that organizations that have suffered from misconduct by management have low internal audit function quality. In addition, employees tend to be more willing to share information with internal auditors than external auditors, which enables internal auditors to help improve audit quality (Burt, 2016).

Governance. A strong nonprofit organization should also have a strong board of directors. This group ideally should be independent from the organization, and not contain members that have been barred by the Securities Exchange Commission (SEC) from serving as board members (Greenlee et al., 2007). In addition, the organization should have a policy that forbids personal loans to board members and executives like policies that the SEC has in place (Greenlee et al., 2007). The board of directors has many important responsibilities, such as creating an audit committee, which can help detect and deter fraud within the organization (Greenlee et al., 2007). Kamaliah et al. (2018) found a significant relationship between good governance and protection from the occurrence of fraud. Therefore, the board should contain members that have the expertise to provide quality oversight for the organization (Sun & Anderson, 2012).

Background Checks. Another important control is background checks. All employees should be checked, but at the very least those that will access to cash or other assets should be reviewed prior to being hired. This ensures that the employee do not have a prior record of questionable activity, which could be a red flag for fraud (Gallagher & Radcliffe, 2002). In the fraud against the American Cancer Society, Wiant stole $7.5 million dollars from the organization, which could have been prevented with a background check (Gallagher & Radcliffe, 2002). Wiant's background check would have showed that he had admitted to stealing $18,000 from a food bank homeless fund nine months prior to his job at the American Cancer Society (Gallagher & Radcliffe, 2002). It would have also shown that he was arrested for check fraud, and that he had served 10 years in prison for credit card fraud (Gallagher & Radcliffe, 2002). Therefore, employee background checks are an important internal control that can help screen against fraud. Background checks should include reference checks, credit checks, education checks, and criminal history checks (Murphy, 2015). This type of due diligence can help protect an organization from unethical employees. Another important control related to background checks is bonding of key employees. Employees that have access to cash or other assets should be bonded to protect against the lost from fraud (Greenlee et al., 2007).

Segregation of Duties. An important internal control that can help prevent fraud is called segregation of duties (Baapogmah et al., 2015). This control ensures that one employee does not have access to both the assets and accounting record of the organization. Authorization, custody, and record-keeping should be handled by different individuals (Gallagher & Radcliffe, 2002). For example, if one employee deposits the cash, writes checks, and manages the accounting records, that employee can steal from the organization and cover it up in the accounting system. Instead it would be better for one employee to handle the cash, another employee signs the checks, and a third employee manage the accounting records. One person should not have significant authority to establish, implement, monitor, and enforce any single function within an organization (Gallagher & Radcliffe, 2002). Segregation of duties can be challenging for nonprofits since many organizations experience relatively high employee turnover (Marks & Ugo, 2020). If segregation of duties is not possible due to not having enough employees, it may be necessary to have an outside accountant or audit committee member be involved in some of the functions, such as reviewing transactions and bank statements (Murphy, 2015).

Monitoring. In addition to establishing policies and procedures for an organization, those controls should be monitored to ensure that they are being enforced. Most fraudsters are first time offenders, so background checks will not be able to filter out all criminals (Johnson et al., 2015). Therefore, employees and volunteers should be monitored, and it should be used to ensure that policies and procedures are being followed. Nawawi and Salin (2018) found an organization that had the proper policies and procedures, but they were ineffective because employees were able to override or disregard the controls. Rubasundram (2015) wrote that training and gradual education can help reduce the override of controls by employees.

Supervision. Another vital internal control is supervision. This control is especially important when segregation of duties is difficult to implement (Chen et al., 2009). Trusted employees in a nonprofit should still have some form of supervision to ensure that fraud is not taking place. Instead of simply trusting the employee, the organization should take a trust and verify approach (Kramer, 2015). There should be a balance between no trust and blind trust (Kramer, 2015). For example, one organization requires that all expenses be approved by a supervisor, as well as the time spent on each project (Baapogmah et al., 2015). Another example is for someone that is not involved with entering accounting information to prepare the monthly bank reconciliation to look for unreconciled transactions, which could indicate fraud (Applegate, 2019). In addition, a manager could review invoices, validate vendors, and confirm receipt of goods before approving check processing (Applegate, 2019). Management can perform bank reconciliations on a surprise basis (Kramer, 2015). At a minimal every organization should prepare an annual budget that is approved by the board and is audited by qualified people at the end of the year (Hill, 2016).

Red Flags. There are several red flags that organizations can look out for to reduce the risk of fraud. Some of the red flags related to billing fraud can include unfamiliar vendors, vendors with post office box addresses, vendors with names that are only initials, and vendors billing more than once a month (Marks & Ugo, 2020). Other red flags may include sudden increases in purchases from one vendor, vendor addresses that match employee addresses, and large billings that are broken into multiple smaller billings to avoid detection (Marks & Ugo, 2020).

Other red flags include employees that are living beyond their means, have financial difficulties, exhibit excessive control issues, or have an unusually close relationship with a vendor (Marks & Ugo, 2020). The ACFE (2020) found that 42% of occupational fraud was committed by individuals who were living beyond their means, and 26% of occupation frauds were committed by those who were experiencing financial difficulties. If an employee begins to show signs of a lifestyle that is more extravagant than their salary can afford, such as jewelry, vacations, and cars, this could be a red flag (Kramer, 2015). The employee who is committing the fraud may claim to have received an inheritance, retirement plan, or spouse raise to explain the purchases (Kramer, 2015). Lenz and Graycar (2016) discussed how the CEO of an organization was able to transfer AUS$ 22 million to his personal account in a major fraud in Australia. A red flag that the fraud was occurring were large material transfers of round amounts to outside bank accounts; one transfer was for AUS$ 3 million (Lenz & Graycar, 2016). These large transfers should have been a red flag to the auditors.

In addition, white collar criminals are typically profiled as friendly, outgoing, and passionate employees that may not appear dangerous on the surface (Marks & Ugo, 2020). They are likely married, belong to a church, have a college education, and no prior arrest record (Kramer, 2015). Employees that are unwilling to take vacation can also be a red flag because they need to stay at work to keep the fraud together (Marks & Ugo, 2020). Mandatory vacation policies should be in the employee manual (Hess & Cottrell, 2016). In addition, employees with addiction problems may commit fraud to feed their addiction and should be viewed as a red flag (Marks & Ugo, 2020).

There are also red flags that organizations can monitor using their data. Transactions that are conducted at unusual times of the day, transactions that occur more frequently than expected or that have large round numbers should be investigated (Marks & Ugo, 2020). In addition, documents that are missing, altered, or that conflict with other documents should be a red flag (Marks & Ugo, 2020). Fitri et al. (2019) found that organizations that had fraud detected had more receivables from related parties and had more frequent changes to auditors. These are some of the red flags that the risk of fraud could be higher.

Anti-Fraud Controls. Over the past decade there has been an increase in anti-fraud controls. There has been a 13% increase in the use of a hotline in organizations; there has also been a 13% increase in the implementation of anti-fraud policies (ACFE, 2020). In addition, there has been an 11% increase in fraud training for employees, and a 9% increase for training for managers and executives (ACFE, 2020). Having anti-fraud policies in place benefits the organization with lower fraud losses and quicker detection (ACFE, 2020). Controls such as having firewall for the organization's server and password protection for the accounting software are two efficient control techniques (Mangala & Kumari, 2015).

Building Fences. In addition to formal laws that are implemented to protect against fraud, Reinstein and Taylor (2017) suggest adding fences to protect against unethical behavior. Fences are unlike laws which have formal punishments; they are communal expectations for behavior that may have negative reputational effects (Reinstein & Taylor, 2017). Reinstein and Taylor (2017) stated that many religious systems, including Jewish people, used fences to keep others from acting unethically. For example, when Adam and Eve were in the garden, God told Adam not to eat the fruit from the tree of knowledge of good and evil (*New International Version*, 1978/2011, Genesis 3). Adam in turn told Eve not to eat the fruit or to even touch it. His recommendation not to touch it is an example of a fence. This recommendation was not a sin, but it was set up to guard against falling into temptation. In the same way Reinstein and Taylor (2017) recommended setting up fences in organizations; the American Institute of Certified Public Accountants (AICPA) has established fences in the form of safeguards to protect against unethical behavior. Fences can help employees choose to act ethically in situations where there are no outright set of punishments. Most internal controls focus on reducing the opportunity leg of the fraud triangle. Fences can help with the rationalization leg of the fraud triangle, which can provide a means to keep employees from justifying that committing a fraud is ok in a particular situation (Reinstein & Taylor, 2017).

Other Best Practices. With the bankruptcy of large corporations such as Enron and WorldCom Congress passed new legislation for public companies called the Sarbanes-Oxley (SOX) Act. Although this law only applies to public corporations, some have considered if these practices should be followed by nonprofits also (Branson et al., 2015). One aspect that some nonprofits have adopted is having a document retention policy (Branson et al., 2015). Branson et al. (2015) found that size of the nonprofit has a significant effect on whether document retention policy is adopted. SOX also makes it a crime to destroy or falsify records or documents to impede a federal investigation (Murphy, 2015). Nonprofits should also adopt similar document retention policies. Garven et al. (2018) found that there has been a spillover effect from SOX in that nonprofit reporting quality has increased since the passage of the legislation. Auditors have changed their audit practices for all their clients leading to an indirect benefit to nonprofit organizations (Garven et al., 2018).

Also, employees and volunteers should also have limited access to the assets and accounting records in the organization. Only those employees that absolutely need to have financial access should have access (Johnson et al., 2015). In addition, purchasing an insurance policy that covers fraud losses is another way to protect against the cost of a fraud loss (Ries, 2016). Oftentimes this is the only means by which an organization can recover losses from fraud (Johnson et al., 2015). Murphy (2015) also recommended fair promotion and compensation practices to deter fraud.

Potential Themes and Perceptions

There are several strategies that nonprofit organizations can implement to reduce the risk of fraud. These strategies are tone at the top, fraud prevention program, and variance analysis. Each of these strategies can help to improve the control environment within an organization.

Tone at the Top. One strategy that can help nonprofit organization mitigate the risk of fraud is the tone at the top. The organization’s leaders, which includes the board of directors and executives, could set the organization’s culture and values. They should model ethical behavior, integrity, and communicate the expectations of ethical behavior for employees (Halbouni et al., 2016). Managers that have outcome bias and are more concerned about the outcome than the means are sending a powerful signal that ethics are not valued at the organization (Hess & Cottrell, 2016). This influence of the organization's culture can have a dramatic impact in the ethical behavior of the employees. There is a link between the culture of leadership and the internal control environment (Baapogmah et al., 2015). Meinert (2016) stated that the fraud leader is more important than technology and processes in understanding where fraud risk is, and how to prevent it.

Campbell et al. (2016) believed the longer the CEO and CFO executive relationship, the less likely the organization will have internal control weaknesses. Higher turnover of these two positions can lead to weaker internal controls. Some studies have also found that spirituality in the workplace can have a positive and significant influence on fraud prevention in an organization (Purnamasari & Amaliah, 2015). These and other measures can help to improve the culture and ethics within an organization.

Fraud Prevention Program. Another strategy that nonprofit organizations should implement is a proactive fraud identification and response program (Marks & Ugo, 2020). This program can help establish the ethical behavior for the organization, close gaps in internal controls, and develop procedures for finding and dealing with fraud (Marks & Ugo, 2020). This program can establish sound practices such as monetary authorization limits, security access controls, and transaction monitoring to limit risk of fraud (Marks & Ugo, 2020). The ACFE (2020) found that organizations that have fraud awareness training are more likely to receive tips of fraud (56%) than those organizations that do not have training (37%). Training is a crucial step towards curbing fraud in an organization (Meinert, 2016; Omar et al., 2016). Kamaliah et al.

(2018) found a significantly relationship between fraud prevention programs and the occurrences of fraud in public agencies.

Oftentimes nonprofit organizations tend to limit the exposure of fraud within the organization. They prefer to keep the incident quiet, dismiss the offender, and limit the damage (Marks & Ugo, 2020). Although this may appear to be in the best interest of the organization, this can also lead to rumors, exaggeration, and more reputational damage to the organization (Marks & Ugo, 2020). Nonprofits should address and deal with cases of fraud promptly and directly to maintain the health and integrity of the organization.

Financial Analysis. One strategy that organizations can use to mitigate the risk of fraud is financial analysis, which involves two steps. The first step is to create a budget for the organization. Not all nonprofit organization prepare a budget. Connolly and Hyndman (2004) found that only 32% of nonprofits prepare a budget, and only 35% prepare a cash budget. Once a budget has been prepared and approved it should be compared to the actual figures at the end of the period. Analyzing variances can help an organization locate the existence of fraudulent or unethical activity (Murphy, 2015).

For example, two of the most common ratios that interested parties analyze are the program spending ratio and the fundraising ratio (Garven, 2015). The program expense ratio is the program expenses for the organization divided by the total expenses (Garven, 2015). This ratio shows how much of the total spending is used for administrative costs and how much is used for carrying out the mission of the organization. The second ratio, the fundraising efficiency ratio, is fundraising expenses divided by total contributions (Garven, 2015). This ratio reveals how much money is spent trying to raise additional funds. Both ratios are analyzed by donors, the media, and watchdog groups to make judgments on the management of nonprofit organizations (Garven, 2015).

Cost Benefit. Although there are many strategies and internal controls that an organization can implement, not all of them should be implemented by all organizations. Decision makers should consider the cost benefit of each strategy and internal control. McMahon et al. (2016) described this as a balance between internal control issues and corporate governance. The organization wants to have security and asset protection on one side of the scale yet wants to maintain fiduciary responsibility on the other side (McMahon et al., 2016). Some internal controls may help to deter fraud, however the cost to implement may not justify the implementation. Spending millions of dollars to prevent a hundred-dollar fraud is not likely to be implemented. The benefit should exceed the cost even if the benefit is nonfinancial. Ahmed and Muhammed (2018) found in their study that organizations that have stronger internal controls are more likely to have significantly higher financial performance. So, there may be some additional benefit to an organization other than just decreasing the likelihood of fraud. In addition, implementing internal controls is not always costly. Some best practices in internal controls come at little or no cost (Frazer, 2016).

Discovered Themes. All of the themes discovered in the findings of this study were discussed in some extent in the literature review. The themes from the field research are: frauds occur, segregation of duties, approval controls, review process, and policies and procedures. The themes also included several policies and procedures that supported the themes, and are: background checks, whistleblower policies, segregation of duties, review of financials, and limited access. Each of these policies and procedures were also discussed in the literature review.

Summary of the Literature Review

No organization is immune to fraud; both small and large organizations have some risk of fraud (Kapardis & Papastergiou, 2016). Nonprofits should strive to build trust in their community. Maintaining community support, maintaining legitimacy with donors, and fulfilling the organization's mission are factors that affect the continuance of a nonprofit organization (Duckles et al., 2005). Nonprofit organizations want to minimize that risk to protect their reputation. A good reputation is one of the most valuable assets a nonprofit organization can have (Gallagher & Radcliffe, 2002). If that reputation is damaged by fraud, it may cost the organization much more than the fraud itself. Trust may be broken, and support from donors and volunteers may be broken as a result. Therefore, it is important for organizations to protect their reputation through internal controls and strategies that can help mitigate the risk of fraud. Prevention is better than the cure; it is better to prevent fraud from taking place than it is to try to detect and stop a fraud (Sorunke, 2016). Organizations should be proactive in dealing with threats of fraud (Ries, 2016). No single control technique will effectively curb the risk of fraud; multiple controls and strategies should be utilized (Mangala & Kumari, 2015). This can be accomplished through internal controls and fraud mitigation strategies.

Transition and Summary of Section 1

Section 1 of this research included the foundation of the study on strategies and internal control procedures for decreasing fraud in nonprofit organizations. This section included the background of the problem, the problem statement, and the purpose statement, which was to research faith-based nonprofit organizations in Texas. Section 1 also included the research questions, conceptual framework, nature of the study, and definition of terms. Assumptions, limitations, and delimitations were then addressed, followed by reduction of gaps, implications for biblical integration, and relationship to field of study. Section 1 concluded with a review of the professional and academic literature.

Section 2: The Project

Section 2 addressed the role of the researcher, the research methodology, participants, the population, and sampling. This section also included data collection, organization, data analysis, reliability, and validity. Each of these concepts were discussed in reference to the purpose statement.

Purpose Statement

The purpose of this qualitative study was to add to the body of knowledge by expanding on the understanding of the factors that lead to frauds being committed in nonprofit organizations. This larger problem was explored through an in-depth study of strategies and internal controls that can help faith-based organizations in Texas. These strategies and internal controls could be used to mitigate the risk of fraud within nonprofit organizations.

Role of the Researcher

In this study, the researcher served as the primary collector, organizer, and analyzer of the data and used the information to report on the findings for the study. Interviews were conducted with workers at faith-based nonprofit organizations to better understand how fraud risk can be minimized. The use of interviews served several purposes. They were used to obtain unique information that is known by the interviewee and to find out about something that cannot be seen by observation (Stake, 2010). Interviews can include open-ended questions that allow the participant to comment or tell stories, which can lead to quotable material (Stake, 2010). The researcher asked follow-up questions for clarity or to better understand a response; however, in semi structured interviewing all of the questions should be uncomplicated and shared with the participants in the same manner (Stake, 2010).

Participants were asked to sign a letter of consent in their participation of the study. Participants were informed that interviews will be electronically recorded to record verbal responses more accurately. The intent of the study was explained along with the confidentiality related to the research. The researcher observed all Belmont Report protocols and sought to maintain ethical standards throughout the study (Office for Human Research Protections, 2021). This study did not involve participation by vulnerable populations and did not require special treatment to accommodate those populations.

Bracketing

The researcher used bracketing to avoid personal bias. Bracketing is when a researcher sets aside his or her pre-understanding of a subject and conducts research in a non-judgmental manner (Sorsa et al., 2015). Without bracketing there is a risk that the research will be biased and only reflect the worldview of the researcher, and not that of the participants (Sorsa et al., 2015). The use of bracketing is important in research. It adds a level of scientific rigor to a study and increases its validity (Chan et al., 2013; LeVasseur, 2003). Research should be conducted in a manner that attempts to remove any and all subjectivity and bias. Researchers should approach a study with an objective perspective in order to provide an authentic perspective from the participants that are involved.

Bracketing can be applied when the researcher discloses his or her past or background with regard to the research (Sorsa et al., 2015). For this study, the researcher is a Certified Public Accountant (CPA) and a Certified Internal Auditor (CIA). He has experience working as an auditor for a Big 4 accounting firm and has worked as a financial administrator for faith-based nonprofit organizations. The prior knowledge and experiences that have been gained from this background was set aside during the interviews so that the participants' viewpoints can be studied. The researcher allowed the participants to answer the interview questions without adding to what was being shared.

In summary, the researcher was the primary collector of data related to the study. He conducted interviews with workers at faith-based nonprofit organizations to better understand how fraud risk can be mitigated. Bracketing was also used to avoid adding personal bias to the study.

Participants

The type of individual that were eligible to be included in this study are those that have financial understanding of the policies and procedures in a faith-based nonprofit organization. These individuals included financial administrators, treasurers, managers, pastors, and other related positions that have some level of financial oversight. These individuals were selected as eligible participants since they have knowledge of the internal controls and fraud risks within the organization. The participants from the organization included both clerical level employees as well as management level employees in order to provide both a detail and overview level of the internal controls.

Research Method and Design

The research methodology includes a discussion on the research method and design that will be used in the study. The method can be qualitative, quantitative, or a combination of both, which is called mixed methods. There are several designs for research which include designs such as narrative, grounded theory, ethnography, case study, and phenomenology.

Discussion of Method

The qualitative method was selected because it was necessary to understand why fraud takes place in faith-based nonprofit organizations. Since this study involved researching two organizations a qualitative method was more appropriate. Stake (2010) stated that most microstudies use the qualitative (or flexible) method, whereas most macro studies use a quantitative (or fixed) method. Since this research was a microstudy, a qualitative method was used.

The qualitative method differs significantly from the quantitative method in several regards. The qualitative method aims to explain whereas the qualitative method aims to understand (Stake, 2010). Since this study aims to understand the strategies and internal controls to reduce the risk of fraud, the qualitative method was the appropriate method for this study. Another distinction between these two methods is the role of the researcher. Quantitative studies involve an impersonal role of the researcher, whereas qualitative studies give the researcher a more personal role (Stake, 2010). Since this study involved personal interviews to gain understanding, a qualitative method was more appropriate.

A third distinction between the two research methods is the type of data that is obtained. Qualitative methods include the study of personal knowledge, however quantitative methods utilize objective measurements (Stake, 2010). Since this study collected personal knowledge from workers at nonprofit organizations a qualitative method was more appropriate for this study.

Discussion of Design

There were several designs that were available when research was conducted using the qualitative method. These designs include narrative, phenomenology, case study, grounded theory, and ethnography. The narrative design is used to study the lives of individuals to better understand the events of their lives (Creswell, 2015). This design was not appropriate for this research since this study was focused on internal controls of an organization, and not the lives of individuals. The grounded theory design is used to create a theory based on data collection using multiple stages (Creswell, 2015). The design would not be appropriate to this study since this research was not attempting to find a new general theory based on data that was collected.

The ethnography design is used to study the shared beliefs, language, and interactions of a cultural group over time (Creswell, 2015). This design would not be appropriate since this study was not attempting to study a cultural group. The phenomenological design is used to study a phenomenon experienced by a group of individuals (Creswell, 2015). Although this design could be used to understand fraud in general, it cannot be used to understand internal controls and strategies to prevent fraud, therefore this design would not be appropriate for this study.

The case study design is used to research an in-depth analysis of one instance of the topic being studied (Creswell, 2015). Case studies are generally focused on one program, event, or organization. The case study design was selected for this study. This was the most appropriate design for this research since this study helps to understand why fraud occurs at faith-based nonprofit organizations, and what are the internal controls and strategies that the organization uses to deter and detect fraud.

Triangulation. Triangulation is needed in research to ensure that the data are accurately collected and understood. The process can be described as looking and listening from more than one vantage point or using more than one data source (Creswell, 2015; Stake, 2010). Having multiple viewpoints can help to substantiate important data. Not all data need to be triangulated. If a statement is something trivial or is a person’s interpretation, there is not a great need for triangulation (Stake, 2010). However, if the data are used for a main assertion in the research there is a stronger need for triangulation (Stake, 2010). Triangulation was used in this study where possible to collaborate the data that was collected. This included asking follow-up questions when a response was unclear or needed to be verified. In addition, responses that were collected were collaborated with other employees or company written documentation where possible.

An additional aspect of validity is member checking. This aspect involves asking a participant if what was written about what he or she said was accurate, and what the researcher heard or seen was correct (Creswell, 2015). Triangulation adds credibility to research and should be used by the researcher. Member checking was used in this study to ensure that the data collecting during the interviews was accurate and correctly portrayed the participants' responses.

The multiple case study method inherently provides a means of triangulation. Findings at one organization could be compared with another organization to check for reasonableness. These findings could also be compared with findings in prior research to check for reasonableness.

Summary of Research Method and Design

In summary, the research method that was used for this study was the qualitative method. The study used a multiple case study design to conduct the research. Triangulation was also used to ensure that the data collected were accurate and properly understood.

Population and Sampling

Determining the population and sample for this study was important in order to define the group that was researched. The population is the entire group that falls within the research target. Sampling is the process of selecting participants or data from the population (Creswell & Báez, 2020).

Discussion of Population

The eligible population for this study was faith-based nonprofit organizations that reside in Houston, Texas, or the suburban areas. These organizations will have 501(c)(3) tax exempt status with the Internal Revenue Service (IRS), and will be listed with the current exempt status on the IRS website. The total number of nonprofit organizations with tax exempt status in the Houston and surrounding areas was 24,204. This number was based on a search on the IRS tax exempt organization search in Houston, Katy, Sugarland, Cypress, The Woodlands, and Brookshire, Texas. This number represents all of the nonprofits in these cities, which includes faith-based and nonfaith-based organizations. Therefore, the number of faith-based nonprofits will be significantly less that the total number of nonprofits. Churches were also included in the eligible population for this study. These organizations are not required to file for tax exempt status with the IRS, therefore they may or may not be listed in the IRS' nonprofit search. The number of churches in Houston was estimated to be over 1,500, which does not include the surrounding area (Church Finder, 2021).

This population size was appropriate for this study since this study seeks to understand strategies and internal controls to prevent fraud in faith-based nonprofit organizations in Texas. Houston and the surrounding cities comprise a significant population in the state of Texas. The Houston metro area has over seven million people and is one of the largest cities in America (Jankowski, 2019). The population of the Houston metro was large enough to contain a significant representation of faith-based nonprofit organizations in Texas.

Discussion of Sampling

Sampling is the process of selecting participants or data from the population for the study (Creswell & Báez, 2020). In qualitative research it is important to select individuals who have experienced the topic that is being researched (Creswell & Báez, 2020). In this study the sample included individuals who had experience with internal controls and strategies for deterring fraud. There are many types of sampling that can be used by the researcher. Creswell and Báez (2020) discussed several of these types, which include opportunistic, convenience, stratified purposeful, random purposeful, and criterion. Each type has potential benefits and drawbacks.

Sampling Method. In selecting a sample from the population for a study a sample can be randomly selected from the population or the researcher can select the participants from the population. A true experiment is when the sample is randomly selected from the population (Creswell, 2015). In many qualitative studies a sample is intentionally selected that will best inform the researcher regarding the research questions under investigation (Creswell & Poth, 2018). This type of sample selection is called purposeful sampling. This method may be selected for several reasons, such as the researcher has access to only some of the population, or some of the population will provide better understanding of the research questions.

In this study a purposeful sampling was used. The researcher selected a sample from the population based on the ability of the researcher to gain access to financial information related to the nonprofit organization. This method was appropriate since not all organizations are willing to share sensitive financial information for research purposes. The researcher selected organizations that were willing to share this information, which required a selection process directed by the researcher.

Sample Frame. The sampling frame is the list of the entire population by which the sample will be drawn (Brasel, 2020). The sampling frame may not match the population the researcher is trying to target. For example, if a researcher is trying to study businesses in

Houston and uses a list of business websites for the population, then the sampling frame will not include business that do not have a website.

For this study, the sampling frame included all faith-based nonprofit organizations in Houston or the surrounding area that were listed on the IRS tax exempt organization search. Since churches are not required to file with the IRS, the sampling frame also included churches that have a website with contact information listed. The sampling frame was also limited to organizations that provide an email address and phone number on their website for contact purposes. This sampling frame was appropriate because an organization should have filed for a nonprofit exemption in order to collect tax deductible donations, and a website was needed in order to find contact information for the organization.

Sample Size. The sample that was used for this study were faith-based nonprofit organizations that were located in the Houston area. This sample was appropriate for this study since the research topic was to study faith-based nonprofit organizations in Texas. The sample size that was used for this study was two faith-based nonprofit organizations in the Houston area. This involved interviewing ten individuals, based on when saturation is reached. This sample size was appropriate because this research was being conducted using the case study design. The case study was centered around the nonprofit organization itself, and the strategies and internal controls that were in place in that organization. Research continued until saturation was reached. Saturation occurs when collecting additional data does not generate additional insight or reveal new information (Creswell, 2015). Interviewing multiple individuals until reoccurring themes began to emerge helped to reach saturation for the study. This included interviewing individuals that had financial expertise in the organization as well as managers and others that were associated with the finances of the organization; interviews were conducted until saturation was reached.

Gaining access to the sample was obtained by contacting the participants through email and phone. The details of the study were shared with the participants, and then permission to interview the sample was sought. Once permission was granted, arrangements for a meeting was made where the researcher could interview the participants using the research instruments that were created.

Summary of Population and Sampling

In summary, the eligible population for this study were faith-based nonprofit organizations that reside in Houston, Texas or the surrounding area that had 501(c)(3) tax exempt status. The population also included churches in the same locations. The sample for this study included two faith-based nonprofit organizations from the populations. The sample was studied until saturation was reached, and where additional research did not yield new insight or further understanding.

Data Collection

This section will address the data collection plan for this study. It will provide an overview of the data that was collected, and how the data were collected. The use of member checking, follow-up interviews, interview guides, and archival data will be discussed. Then the data organization plan will be outlined, which will provide an overview of how the data were organized for the study.

Instruments

There are several instruments that can be used to collect data for research. Interview guides, surveys, and archival data are valuable instruments for collecting data. Each of these instruments have important advantages and disadvantages depending on the type of data that were being collected.

Interview Guides. An interview guide was used to conduct the interviews for this study. The guide is located in Appendix B and contains the questions that were asked in a semi-structured interview format. The first two questions in the interview guide ask for the participant's name, position, and duties in the organization to establish a basic understanding of the participant. The third question asks the interviewee what are the strategies that the organization uses to lower the risk of fraud. This question was used to understand the high-level strategies that the organization had in place to mitigate the risk of fraud. This question was directly related to the research topic and RQ2 regarding strategies to reduce the risk of fraud.

The next question asked how the organization was able to assess the effectiveness of the strategies to lower the risk of fraud. This question was designed to determine if the strategies that are implemented are effective and enforced, and also help to answer RQ2 with regard to fraud strategies. The fifth question sought to understand the practices and policies that the organization uses to prevent or detect fraud. This question was used to move from the high-level strategies to medium level practices and policies to help deter fraud. Determining if the organization used these practices helped to answer RQ3 related to which practices faith-based organizations in Texas use to deter fraud.

The sixth question asked the participant what type of internal control processes the organization has to detect or prevent fraud. This question was used to understand at a more detailed level the internal controls that the organization has implemented. This question had three follow-up sub-questions to further explore this question. The first sub-question asked about a process for collecting revenue, donations, or gifts. Understanding this process would illustrate the types of internal controls that the organization used on the cash receipts side of their accounting system. The second sub-question inquired as to the process for making payments with cash, check, or electronically. This question sought to understand what internal controls were in place on the cash disbursements process. The third sub-question involved controls related to accounting data and reporting. This question was used to address internal controls connected to the accounting software and other related activities. This question and the subsequent sub-questions are related to RQ2, which sought to understand internal controls that could be used to mitigate the risk of fraud.

The seventh interview question asked if the organization had experienced inadvertent use of funds, funds used incorrectly, waste, or fraud within the past ten years. This question was used to see if there has been an activity that could indicate a possible fraud within the organization. This question helped to answer RQ1, which sought to understand the factors that could lead to an increased risk of fraud within an organization. The eighth interview question also sought to answer RQ1, and better understand the factors that could lead to fraud. This question inquired what strategy or internal control the interviewee believes had been the most successful in detecting and preventing fraud. This question was more subjective; however, it allowed the interviewee to share insight from their experience in using strategies and internal controls to detect and deter fraud. The answer to this question could be valuable in determining the most important tool that other organizations can consider when designing their own policies and procedures.

The next question asked what strategies or internal controls the participant believed their organization should implement to further deter and detect fraud. This question allowed the participant to share any strategies or internal controls that he or she would like to implement in the future but had not been able to because of a lack of time or resources. This question would help to better understand RQ3 related to faith-based organizations in Texas, and the future plans they had with regard to preventing fraud.

The final question asked if there was any additional information that the interviewee would like to share that has not already been discussed. This question allowed for the respondent to share anything that he or she felt was important to the research, that was not asked directly through one of the previous questions. This final question could be related to any of the research questions depending on what the participant shared in his or her answer.

Surveys. Prior to the interview a pre-interview survey was sent to the participant to gather some initial information for the interview. The survey questions can be found in Appendix A. The first eight questions asked for information related to the participants to better understand the role and experience of those who were interviewed. There are questions to determine the amount of work experience the participants had with nonprofits, and the total experience they had in their field (e.g., accounting). There were also questions regarding the participants education level and advanced certificates, such as Certified Public Accountant (CPA) to determine their level of understanding in the area of finances.

The last two questions focused on the internal controls of the organization. Question nine had six sub-questions to determine which practices and policies the organization used. The sub-questions asked if the organization had any of the following: a code of conduct, a whistleblower policy, an annual external audit, and internal audit department, a fraud control policy, and an assessment of the risk of fraud. These questions were designed to help the researcher determine which areas to focus on during the interview. For example, in the pre-interview survey participants are asked if their organization has a whistleblower policy. If they answered yes in the survey, then they would be asked to explain how the policy works during the interview.

Archive Data. Archival data were used prior to the interviews to gain an understanding of the financial condition of the organization. This archival data included prior financial statements, annual reports, tax returns (Form 990), and other documentation publicly available from the organization. Studying prior financial data could help answer the research question regarding the factors which increase the risk of fraud within an organization. Studying the financial statements after a fraud could help to understand the financial impact of the fraud.

Archival data were also used if provided by interviewees in response to an interview question. For example, if the interviewee was asked about policies and procedures related to internal controls, and the interviewee provided the researcher with a copy of the organization's policies and procedures, then this document would be retained for the research, and could be used for triangulation purposes.

Data Collection Techniques

The researcher had prepared a data collection plan containing an overview of what data were collected and how the data were collected. Data were collected through semi-structured interviews with participants from faith-based nonprofit organizations in Houston, Texas, and the surrounding area. This data were collected from purposely selected organizations to better understand the research problem and questions (Creswell, 2015). The interviews used semi-structured interview guides, and follow-up interviews for member checking and any additional questions that arose from the initial interview. The use of semi-structured interviews was appropriate for this study since this form of inquiry helped the researcher better understand what strategies faith-based nonprofit organizations used to detect and prevent fraud. Semi-structured interviews were also appropriate because it allowed the participants to explain a topic in their own words, with more elaborate explanations than those that are found in structured interviews (Yin, 2016). This provided a richer understanding of the research problem and related questions.

Member Checking. Member checking is the process of taking the final report back to the participants to verify that what was said was accurately recorded in the study (Creswell, 2015). In this research member checking was used to determine if the participants felt like the information they provided was accurately portrayed. This was performed by sending the final report back to the participants for review. The interviewees had an opportunity to correct any inaccuracies in the report. Those changes were incorporated into the final report.

Follow-up Interviews. The initial interview responses with the participants led to new interview questions. These additional questions were asked if the researcher believed that they would add to better understanding the research questions in the study. If these additional questions are simply clarifying questions to the original interview guide, these questions were not be added to the interview guide. However, if the additional questions were new questions that were not related to the original questions asked in the interview guide, then these additional questions were added to the guide. If these questions arose after the interview has ended, the researcher considered scheduling a follow-up interview to ask these additional questions.

Data Organization Techniques

Data from this study were organized to enhance the ability to analyze the data, sort the data into themes, and to identify emergent ideas. Interviews were audio recorded electronically using an app and then transcribed into a document. The participants' names were masked to protect their identity (Creswell & Poth, 2018). Participants were numbered 1, 2, 3, and so on, to protect their identity. Raw data from this study were stored on a password protected, separate, portable electronic storage device. The raw data will be stored for three years after the completion of the study, after which time the data will be destroyed to protect the participants' confidentiality. This was an appropriate process for data collection and storage as it mirrors the consent forms that the participants agreed to for the interviews.

The data collected were organized using NVivo software. This software allowed the researcher to organize all of their work in one location. Various types of research can be organized including pdf files, images, videos from interviews, survey results, and spreadsheets. This software also has the ability to import many other files types including emails, Evernotes, Survey Monkey, and many others.

Summary of Data Collection

In summary, data were collected through the use of semi-structured interviews with participants from faith-based nonprofit organizations in and around Houston, Texas. Member checking and follow-up interviews were used as needed to ensure accuracy. Data were then organized and stored for analysis.

Data Analysis

This section will provide an overview of how data will be analyzed in the study. It will include a section on the process for reading and memoing emergent ideas and classifying codes into themes. The process for developing and accessing interpretations will be discussed, followed by the process for representing and visualizing data. Then the plan for conducting analysis for the triangulation of the interview data will then be examined.

Coding Process

After the interviews had been conducted the recorded audio was transcribed into a written document. Agar (1980) suggested that the researcher should read over the transcription several times to gain an understanding of the interview as a whole. After transcription and initial readings, the interviews were read, and emergent ideas were recorded using memoing. Memos in this context are ideas, short phrases, or key concepts that the researcher records in the margins of the transcription (Creswell & Poth, 2018). As emergent ideas were discovered by the researcher they were recorded as memos in the margin of the interviews.

Coding Themes. Once the researcher finished memoing the data, the memos was organized into categories or codes. Coding is the process of aggregating the data into smaller categories of information and assigning a label to the code (Creswell & Poth, 2018). Each code was listed in the codebook. The codebook consisted of the name of each code and a shortened label to apply in the margin; a description of the code was listed, and an example of the code from the study was listed (Creswell & Poth, 2018). This study utilized lean coding, which begins with five or six categories, and then expands the list as review of the data continued (Creswell & Poth, 2018). The final list of codes for this study was less than 20 codes.

Interpretations. After the coding process the researcher developed and assessed interpretations. Interpretations involve moving from the codes to finding the larger units to make sense of the data (Creswell & Poth, 2018). It involves using strategies to find summaries, locate patterns, develop stories or summaries by answering questions such as what information is unusual or interesting to audiences and participants, or what are the dominant and alternative interpretations (Creswell & Poth, 2018; Grbich, 2013). In this study interpretations were developed using these strategies to help uncover the larger aspects of the data.

Data Representation. The next stage of data analysis was data representation. Stake (1995) outlined four types of data analysis for case studies. One type of data analysis is through a visual image of the information (Creswell & Poth, 2018). This can be in the form of a table, a diagram, a matrix, or other visual image. When two or more cases are studied Yin (2018) advocated that researchers can use cross-case synthesis to analyze the information.

Data representation and visualization can be depicted using software. NVivo is one such software that is used for qualitative analysis. The researcher used this software to organize, analyze, and visualize the data. This software was also used for memoing, coding themes, and interpretations throughout the study.

Analysis for Triangulation. As discussed earlier, triangulation is the process of using different and multiple sources to provide collaboration for the accuracy and validity of the study (Creswell & Poth, 2018). This study utilized triangulation by interviewing several employees at a nonprofit organization to help collaborate the data that was being gathered. Triangulation also occurred by comparing written documents, such as archive data obtained from the organization, with data obtained through interviews.

Summary of Data Analysis

In summary, data analysis involves discovering emergent ideas, coding themes, finding interpretations, and creating data representation. These steps of the research were aided by using qualitative analysis software, such as NVivo, to work through these processes more efficiently. In addition, analysis for triangulation was used to ensure that the data were collaborated for accuracy and validity.

Reliability and Validity

This section will provide an overview of the reliability and validity for the study. A discussion of how reliability will be ensured will be discussed, which includes dependability, transferability, credibility, and confirmability. The several aspects of validity will also be addressed, which includes triangulation, bracketing, and saturation.

Reliability

In qualitative studies reliability is when the researcher checks the accuracy of the finding through the use of various procedures (Gibbs, 2007). There are several terms that are used to enhance the reliability of a study; these terms are dependability, transferability, credibility, and confirmability (Lincoln & Guba, 1985). Dependability is being able to rely that the results are not subject to change or instability (Creswell & Poth, 2018). Dependability was achieved by interviewing individuals with knowledge of the organization's accounting systems and triangulating that data with other individuals. Credibility involves conducting research such that the researcher is confident about the interpretations, observations, and conclusions that are made and that the weight of evidence is great enough to become persuasive (Creswell & Poth, 2018). This study achieved credibility through obtaining multiple sources of data to provide a substantial level of evidence. Confirmability is the ability to corroborate that data are accurate through an alternative source. Data from this study were confirmed through triangulation and saturation of the data. Transferability refers to the ability to use data in one study and apply it to other research. Transferability was obtained by comparing findings to other nonprofit organizations in the literature.

Validity

Validity in qualitative studies occurs when the researcher's approach is consistent with different projects and different researchers (Gibbs, 2007). There are several validity strategies that a researcher can use to enhance the validity of the research. Bracketing, triangulation, and saturation are three strategies that can increase the validity of the study. Bracketing, or sometimes referred to as epoche, is when the researcher sets aside all preconceived experiences to better understand the experiences of the participants (Moustakas, 1994). In this study the researcher set aside prior experiences as an auditor and accountant and conducted data analysis of the participants to better understand their experiences.

Another strategy for enhancing validity is triangulation. This is the process of using different and multiple sources to provide collaboration for the accuracy and validity of the study (Creswell & Poth, 2018). This study utilized triangulation by interviewing several employees at a nonprofit organization to help collaborate the data that are being gathered. Triangulation also occurred by comparing written documents obtained from the organization with data obtained through interviews.

A third strategy for enhancing the validly of a study is saturation. Saturation is the process of obtaining more data and information, until the researcher reaches the point where he or she no longer finds new information that adds to the understanding of the study (Creswell & Poth, 2018). In this study saturation was used through the use of multiple interviews with nonprofit organizations. Ten interviews were conducted, until the researcher reached saturation, and no new understanding was obtained through additional interviews.

Bracketing. As previously discussed, bracketing is when the researcher sets aside all preconceived experiences to better understand the experiences of the participants (Moustakas, 1994). It is when a researcher sets aside his or her pre-understanding of a subject and conducts research in a non-judgmental manner (Sorsa et al., 2015). The researcher used bracketing in this study to prevent bias from influencing the findings. Bracketing was used to prevent the researcher from anticipating themes that will emerge from the findings. The researcher approached the data from a nonbiased vantage point, without any preconceived ideas as to the themes that may or may not emerge from the data.

Summary of Reliability and Validity

In summary, reliability and validity are important concepts that will be used in this study. Reliability involved ensuring that the findings have credibility, transferability, dependability, and confirmability. Validity was achieved through the use of bracketing, triangulation, and saturation. Each of these tools added to the overall reliability and validity of the study.

Transition and Summary of Section 2

Section 2 discussed the role of the researcher, the research methodology, participants, the population, and sampling. This section also addressed data collection, organization, data analysis, reliability, and validity. These concepts were discussed as they related to the purpose statement of this study.

Section 3: Application to Professional Practice and Implementations for Change

Section 3 included a discussion of the overview of the study and the presentation of findings, which included discussions on the themes discovered, interpretation of themes, representation and visualization of the data, relationship of the findings, and a summary of the findings. This section also entailed the application to professional practice, which showed how this study can improve general business practice and potential application strategies. Recommendations for further study were then be shared followed by reflections, which included personal and professional growth as well as the Biblical perspective of this study.

Overview of the Study

This study involved researching strategies and internal controls at faith-based nonprofit organizations. Organizations were contacted to gain permission to conduct the study. Once permission was granted, individual employees were given a pre-interview survey to complete as shown in Appendix A. This survey was designed to gain an understanding of the level of experience of the participant and the general internal controls used by the organization.

Individual interviews were then scheduled with each of the participants. Each interviewee was asked all of the questions listed in Appendix B. Their responses were audio recorded and then transcribed. After transcription, the interviews and pre-interview surveys were uploaded to NVivo for data collection and analysis purposes. Archival data were also gathered from the organizations regarding their financial data as reported to the Internal Revenue Service (IRS) and uploaded to NVivo. The data were then coded based on themes that emerged from the participants. These codes were further organized into smaller categories and annotations were added to develop themes from the interviews. The transcriptions and archival data were used to compile the findings from the study. The findings were also member checked for accuracy and reliability.

Presentation of the Findings

This section will discuss the findings from this study. It will include the themes that were discovered throughout the research, the interpretation of those themes, and both representation and visualization of the data. In addition, the relationship between the findings and the research questions, conceptual framework, anticipated themes, the literature, and the problem will be discussed.

Themes Discovered

There were several themes discovered after conducting the field research. These themes are frauds occur, segregation of duties, approval controls, review process, and policies and procedures. Each of these themes will be discussed individually.

Frauds Occur. One of the major themes was that frauds occur. All of the organizations studied had some reported fraud. One organization experienced a major fraud. One employee stated plainly "we have been the victim of fraud" (R6). A former employee fraudulently signed for his supervisor, and he created fake receipts. This employee was able to steal nearly one and a half million dollars from the organization over a 10-year period. He used this money to dine out at expensive restaurants and to go on many vacations. People thought he was traveling for mission purposes when in reality he was going on vacations in cities and countries that were not where he said he was going. This fraud became one of the largest frauds against a church in the state of Texas. The perpetrator was prosecuted, was found guilty, and sentenced to prison.

Another instance of fraud was related to tips being stolen from the tip jar at a restaurant on the organization's premises (R1). The factor that led to this attempted theft was unsecured cash. Since the cash was not in a locked drawer, it was at risk of being stolen. The cash was at risk because it was not being monitored by either a camera or an employee.

Another attempt of fraud against the organization was the submission of fraudulent checks for payment (R3). These checks were stopped by an employee in the organization prior to being paid by the bank. The factor that would have allowed this fraud to occur would be a lack of an approval process by the accounting department. Having this approval process in place was an internal control that protected the organization from fraud. Another organization from the findings also experienced an attempted fraud through an illegitimate check (R7). The fraudster obtained a check from the organization, washed it in order to alter it, and then took it to Walmart and made an electronic payment at one of the registers. The employee stated that “even with everything in place that we had in place with positive pay, they’ll find a way if they’re determined enough” (R7).

Another fraud that was shared by one of the organizations was in the culinary area (R8). The administrative assistant for the culinary department was making the deposits for the revenue that was collected. The organization believed that she had stolen over $30,000 from the organization over several years. She accomplished this by skimming some of the cash off of the deposits before bringing them to the bank. A trend analysis of the revenue quickly showed that there was an issue, but lack of evidence prevented the organization from prosecuting.

One of the organizations also detected a fraud related to its Automated Clearing House (ACH) process (R9). The perpetrator contacted the organization using a known vendor email address. The fraudster gave the organization the routing number and account number for sending the funds. The organization sent the funds and then afterwards realized that the vendor’s email account was hacked, and that the routing number and account number belonged to the fraudster.

After this incident, the organization added a policy to call the vendor if there was a request to change ACH payment information.

Another fraud that was shared was related to purchasing fraud. An individual would purchase an item, receive reimbursement from the organization, and then return the item (R10). This allowed the perpetrator to pocket the cost of the item. Consequently, the organization cut out all personal reimbursements.

Lessons Learned. There were several lessons that were learned from this study. The first major lesson learned was from the executive pastor, who shared four factors that contributed to the major fraud (R6). The first factor was that the fraud was committed by a trusted individual. This individual was the person that people would least expect to commit a fraud. This individual was someone who taught Sunday school, preached in the pulpit, was perceived as a close friend with the Senior Pastor, was the son-in-law of an influential person in the church, and was a long time staff member of the organization. Another person said he was a long-term employee who was well liked, charismatic, and very outgoing.

The second factor that contributed to the fraud was access to funds (R6). This individual was the primary staff member responsible for the disbursement of the church's mission fund. This large fund was meant to be used each year to fund missions around the world. This individual had access to these funds and was able to use them for personal expenses instead of ministry related uses by "forging his supervisor's signature, deceiving the Mission Council, creating false documents, and continually covering his tracks" (R6).

Another factor that contributed to the fraud was the individual's "willingness to lie and use deceit" (R6). He would use lies, intimidation, and other methods to perpetrate the fraud. The last factor discussed was social manipulation. He became best friends with his supervisor in order to build up trust. He took one of the employees from the business office on mission trips with him in order to manipulate them. He would also use manipulation if anyone tried to question what he was doing. “He really used the guilt trip of ‘I’m out on the mission forefront. I’m sweating in India. You’re sitting here in an air-conditioned office. How dare you question anything I did’” (R6).

Another major lesson learned from this study were the possible reasons why a major fraud was able to be perpetrated in an organization. One of the other possible reasons that the fraudster was able to perpetrate this fraud was due to the naivety of the staff. One employee stated, “I didn’t think he was the wolf because I don’t think like that” (R7). Another employee stated that “I was wildly naïve. I would have told you there was no way in a million year somebody could take a million dollars from our church and I would have believed it to the core of my being” (R8). He added,

> there are people that do have sin problems in certain areas that you don’t…like I don’t think about taking a penny from this church. And unfortunately, that can make you naïve. So, I think that people that don’t have a sin problem with being a thief can naively assume it’s not happening. (R8)

He added, “We had no idea, no clue what was happening” (R8).

The perpetrator was also able to get away with the fraud because some of the internal controls were not effective. “We lost control of the process for whatever reason. He wasn’t under the same scrutiny as everybody else” (R8). The trust factor and manipulation factor provided a means for the perpetrator to carry on the fraud.

A participant shared his thoughts regarding the ability to commit fraud. He said that "little fraud can happen with someone being negligent. For example, if a manager doesn't review some work there can be an opportunity for a small fraud to occur" (R8). He went on to say that

> big fraud, six-figure fraud…depending on the size of the organization has to have some help. You have to either have someone who looks the other way and doesn't want to ask questions and doesn't want to know answers, or you have someone with you who knows what's going on and failed to report it. (R8)

He reiterated by saying

> Now you can have negligent fraud in any organization, small amounts because of negligence, just people not doing their job and getting in a hurry. Big fraud requires involvement of someone beyond the perpetrator in that is either looking the other way and not asking questions or knowing and not reporting. (R8)

A third major lesson learned from this study were the red flags related to the frauds. When asked about red flags related to the major fraud the business office did not see any red flags related to creating false receipts and stealing money (R8). Some staff had concerns about the perpetrator unrelated to the money. For those that did not know the perpetrator they would think he was living within his means because he lived in a two-bedroom condo near the organization. However, those that were close to him would have noticed that he ate at very nice restaurants frequently and was always going on vacation. Those who were aware of the perpetrator being extravagant saw his extravagance having ministry linkage, which may have led some to dismiss it as a red flag.

When asked what strategies or internal controls you believe have been most successful in detecting and preventing fraud, the director responded that it is transparency and accountability

(R8). Transparency for this organization occurred when the business office opened up the financials to more people, so that more eyes could be review what was happening with the finances. In addition, accountability transpired when the immediate supervisors had to approve every expense and levels of approval where added to every purchase that was made. These and other examples have added to the transparency and accountability of the business office to the organization.

Frauds against nonprofit organizations can do severe damage. One employee stated that some people still have not come back to church after the major fraud was revealed. Another stated that “it was pretty damaging to us a church, as far as people go. The money’s recoverable, but it was pretty damaging emotionally” (R7). The employee added, “It was pretty rough. I mean, you see this person as one way…so at the time it was really, really, really rough” (R7). The Director added that “it was one of the most gut-wrenching things that everybody has been through…people are still recovering” (R10).

Employees now realize that fraud can occur in every organization, even in faith-based nonprofit organizations. One of the employees stated that “at the end of the day a person who’s determined enough and smart enough will be able to perpetrate a fraud. The question is, ‘how long will it go and how much will it be’” (R6)? He also said that “there’s always going to be deceitful people, wicked people that are going to figure out a way to steal money…as a nonprofit, a steward of God resources, got to figure out a way to catch them” (R6). Another employee stated that even with all of the new controls in place “It can still happen if people are determined enough to do it” (R7). The employee added, “You just have to be aware that it’s going to happen and then pay attention” (R7). One employee summarized the fraud investigator by saying, “you know, it’s happening in every nonprofit. It’s just a matter of how much, and is it getting caught" (R8)? No organization can completely eliminate the risk of fraud. However, lowering that risk should be a permanent goal for nonprofits.

One employee stated

> we ignore red flags, so pay attention to the flags in general and listen to the people when they make them. I think that those are going to be your biggest things, because all the other things in play can get bypassed if you're ignoring them. (R7)

Another employee warned

> one of the interesting things about fraud is it can go right by you if you're not aware, if you're not in the ministry or the operation itself. You can be fooled pretty easily with fake receipts and fake signatures. (R8)

The employee had this to say about fraud, "It happens. Unfortunately" (R8).

Segregation of Duties. Another major theme from the findings was segregation of duties. Segregation of duties was a type of internal control where multiple employees are given a part of an accounting process as a means to decrease the risk of fraud (Baapogmah et al., 2015). Segregation of duties was a type of internal control that was employed by one of the nonprofit organizations that was interviewed.

For example, one employee stated that she is responsible for the bank reconciliation, fixed assets, and depreciation, however she does not sign the checks (R2). She said, "their duties do not overlap; if someone makes the deposit, they should not be the one processing the deposit." Another interviewee in the organization, renamed Stephanie, stated, "Heather opens the mail and does the deposits, she [Stephanie] can't take them to the bank" (R3). Stephanie also mentioned that since she does accounts payable, she does not reconcile accounts payable. Heather reinforced that segregation of duties is in place by stating that they try to divide things up so that multiple employees are involved in the collection and payment processes (R4). For example, since Heather records the deposits, she does not take cash to the bank so that one employee does not have access to the assets and records in the collection process.

Another organization also shared that they use segregation of duties in their business office. “We do have some segregation of duties. Kim is the point person for cutting checks. All of the checks get a manager’s approval before they get to Kim” (R8). He went on to say that he or the director of finance releases the checks after review and approval. “And then once the checks are cut, we have a register that we then review with the checks when we sign off,” the employee added (R8).

Although segregation of duties was a strong method for mitigating the risk of error and fraud, it is not always possible. One organization said that this is sometimes difficult for organizations that have a limited number of employees (R1). The controller stated that, “we try not to overlap our critical functions, which is disbursements and receipts” but in other areas there are at times some crossover (R1). This crossover which cannot be prevented due to the small size of the accounting department, “we try to cover that by having review in place” (R1). Review or supervision is a method to compensate for lack of segregation of duties. If one employee is doing a task that normally would be conducted by two or more employees, having a second employee or manager review the transaction is a compensating control that protects the organization.

Employee Rotation. In addition to segregation of duties organizations can sometimes detect fraud by having employees rotate duties, or by making employees take their vacation time. Since some frauds can only be concealed by constant manipulation, having employees take a break from a responsibility can sometimes uncover a fraud. One organization uncovered a major fraud when a different employee started reviewing the expense reports (R6). The fraudster had been "circumventing his supervisor and he had intimidated our financial services director, not to question him" (R6). When the financial services director went to another job, and the supervisor was out of the country a different employee was responsible for approving the fraudster's transactions. This employee asked the fraudster to explain his credit card charges. Although the fraudster attempted to conceal his fraud by saying, "How dare you question me," this employee was a factor to uncovering the fraud (R6). He added, "So it was really human eyes, a fresh set of eyes looking at it. And I think that's why you can't depend on one person…there's always gotta be two or more" (R6).

Approval Controls. Another major theme that was identified from the fieldwork was the use of approval controls. These types of controls are policies and procedures that require approval from either an employee or manager for an action to be taken. For example, one of the organizations uses approval controls for their disbursement process (R1). They have set limits on how much one employee can disburse for payment. At the base level, the accounting manager will initiate the process, however if the disbursement is over one thousand dollars, two officers must approve the transaction. Furthermore, if the transaction is over five thousand dollars the Chief Operating Officer (CEO) must also approve the transaction. This level of tiered approval helps to "guard the gate" as described by the controller at this organization (R1). It prevents one employee from accidentally or fraudulently paying a large disbursement, which would lead to a large financial loss for the organization.

Approval was also used by an organization for spending limits. One of the managers stated, "we have spending limits for each credit card. If a single purchase goes above their limit or the monthly accrual, they have to get permission from their supervisor" (R6). The manager also reviews and approves each credit card charge to ensure there is a proper receipt for the purchase. The receipts are scanned and available for review digitally through the accounting software.

Another approval type control was an approval process used by one organization to approve check disbursements (R3). The organization has an internal control where all check payments must be approved by the accounts payable department before the bank will process the check. This control is called positive pay, and it is designed to prevent fraudsters from submitting fraudulent checks for payment. One organization said that this control was very effective and has prevented check fraud from occurring. The accounts payable employee stated that she found, “several checks in the past that [had] numbers not in sequence, and you could tell signatures were forged” (R3). When these fraudulent checks were detected they would be brought to the attention of the controller, who would determine if the checks were indeed fraudulent. If the check was determined to be fraudulent, it would be returned to sender. Without the positive pay internal control in place these fraudulent checks would have been processed, and then the organization would have to spend time and money attempting to retrieve those funds. Another organization that was interviewed stated that they also use positive pay (R9). This organization has a manager approve check disbursements, and a second manager approve all check disbursements above a certain threshold. In total there are “three levels of approvals before any checks be cut” (R9). This provides multiple checks and balances to ensure that only legitimate checks are issued. An employee confirmed this by stating “we’ve created multiple levels of approvals and oversights and they’re all electronic, so we can track anybody who’s entered and approved” (R10). This online approval system is used to replace a manual system that was ineffective. “We needed to get away from the manual signature as some of those were copied and forged” (R10).

One organization also uses approval type controls with transactions related to student banking (R4). Two signatures are generally required to remove funds from a student's account, or to use the funds to pay the student's tuition fees. In addition, wire transfers also require two signatures for processing. This process helps to minimize errors and fraud that could occur.

Several other employees echoed that the approval controls were foundational within their organization. One employee stated that, "one of us initiates and the other approves" (R5). Another employee stated that there is "an administrator that, you know, oversees everything…" (R2). Another mentioned that all checks are reviewed by one of the managers before getting approved (R1). There are other procedures that also require signatures for approval. For example, to sign a contract that extends beyond the fiscal year the executive pastor has to sign, in addition to the employee's Designation of Authority (DOA; R9).

Although the approval process can be a strong internal control against fraud and error, it is not without weaknesses. The director of operations at one organization stated that he was concerned that managers could approve transactions without first reviewing them. "Managers too readily can click on their approval" (R8). He believes that the organization should do more testing to ensure that the credit card transactions have been properly recorded and that employees are following the organization's policies and procedures.

Approval type controls are only as good as the managers that grant the approvals. The director at one organization stated that they moved from a manual approval process to an online process (R8). Under the manual format a manager could look the other way and not necessarily approve an expense. This new format forces managers to participate in the approval process. Without the manager's approval the transaction will not be recorded. The benefit is that the manager must approve all transactions, however the weakness is that "it's easier for managers to review things quickly. It's easy to click, click, click" to approve a transaction (R8).

Another employee reiterated the importance of management oversight. "I think probably one of the biggest things is making sure that the managers do what the managers are supposed to do" (R10). She stated that some managers do not want to get involved in accounting or get annoyed by having policies to follow because they want to focus more on the ministry aspect of the organization. However, "if the manager who are responsible to approve things don't actually take the time to review and approve this all falls apart" (R10). Management approval is a major internal control, without which, the entire control environment is jeopardized. "That is my only thing…I don't know how to stress to managers how important it is…to get them to do what they need to do" (R10).

Background Checks. An approval type control that was used at one of the organizations that was interviewed are background checks (R4). This organization conducts background checks of potential employees at the point of employment. The human resources department was the one who conducted the background check as part of the onboarding process. One of the employees at the organization conferred that a background check was conducted on her prior to her employment. She shared the longevity of this practice with her statement, "Background checks on new hires…I've been here for twenty-two years, so it was a long time ago that I got mine…" (R4). This type of control helps protect an organization from hiring an employee that may be more susceptible to committing fraud. Another organization that was studied also uses background checks as part of the hiring process (R6). These checks alert an organization to employees that might be more susceptible to committing fraud prior to being hired.

Review Process. Another major theme from the study was the review process. This process involves having an employee or outside party review transactions within the organization. The review process was a major theme that was used at all of the organizations that were studied.

External Audit. The primary review process used by one organization was the annual audit. This organization hires an outside, independent accounting firm to perform an audit on the financial statements. Every employee at one organization discussed the audit (R1, R2, R3, R4, and R5). One employee stated that there is an, "external audit every year" (R2). Another mentioned, "an audit every year," and a third said that there is an "annual audit" (R3 and R5). One employee stated that having an audit was beneficial for the organization because, "they can come in and see things that, you know, we internally don't see, and they ask about it" (R5). The auditors are able to look at policies and procedures from an independent outside prospective, which can help the organization improve their controls. The organization also relies on the annual audit to help detect fraud. One employee emphasized this by stating, "Well, the external audit…if there's any fraud, we would hope that they would be able to detect it" (R2).

Internal Audit. In addition to have an external auditor, one of the organizations also utilized internal auditors. They "engaged an internal audit firm that is going department by department weighing risks" (R6). The organization said that after a fraud was found "we were spending a great deal of money on an outside internal audit firm that comes in and looks over every single process" (R6). In addition, a forensic accountant was hired to go through the entire system to see how the fraud was committed. They determined that the fraud was the product of one person acting alone. After the internal auditors assessed the risks of the organization the external auditors were used to review everything.

One organization stated that they have an annual external audit, use internal auditors, and have a finance committee that reviews the policies and procedures and financials (R6). One of the staff stated that they have been conducting an audit for years (R8). The nonprofit feels that if they have enough people looking at the financials the likelihood of finding something will be greater. They have even had the internal auditor conduct a risk assessment to ensure that there are proper segregation of duties, and that all of the different pieces of the organization are properly separated. In addition, they have audit reports that can be run from the accounting software that the organization uses.

Having various levels of review is important, however it does not guarantee fraud will not occur. An employee mentioned that even though they did a lot of review in their business office, the review was not good enough to catch a fraud that was taking place (R8). Therefore, one employee stressed that they need additional review in their office, even though the internal auditors believe that the updated level of review is sufficient.

Internal Review. In addition to external and internal auditors one organization used internal review to further increase the level of review of the financial statements. Historically they distributed their financials to all of the administrators and directors, as well as the ministers and director's assistants. The recipients of these financials did not always do much with this information. "I think a lot of times they filed it away. I think managers and directors just didn't pay attention" (R8). After discovering a major fraud, the business office decided to broaden the access of the financials so that more people could review them. During the fraud, the fraudster did not want everyone to have access to the financials. The fraudster "kind of used access to financials like a power tool. They didn't want everybody to have access to the financials" (R8). Therefore, the organization is taking an opposite approach in the post-fraud environment. "I think everyone should have, short of people's payroll, free access to everything" (R8). He went on to say, "I'm convinced that the more people we distribute the financials to the better" (R8). Now many more employees have access to go online and review the financials for themselves. The Director of Operations said, "it gives people opportunity to raise their hands, say something's not right here" (R8).

Policies and Procedures. The last major theme that was discovered is the policies and procedures that the organizations have in place. These policies and procedures provide several types of internal controls that help an organization mitigate the risk of error and fraud. They can also be divided into several categories.

One organization interviewed has a process for making purchases. They use a purchase order policy. Purchase orders must accompany an invoice and supporting documents before being processed by accounts payable (R1). Approval must be made before payment can be made. Another employee confirmed this process by stating that there is a "full procedure where there should be a purchase order for most things. It has to be approved and then processed for payment" (R2). A third employee stated, "if a bill come in…there has to be a purchase order for the actual purchase to be made" (R3). They went on to say, "there are certain restrictions to the value of the purchase, whether who needs to approve it or how many approvals we need to get" (R3). If the payment involves an Automated Clearing House (ACH) or wire transfer, one employee will create the template for the transfer, and another employee will approve it. An invoice or some other document must accompany the payment for it to get processed.

Another organization uses a different strategy for their purchasing process. Historically, this organization used a reimbursement process for its employees (R8). They used what was called cash in advance of expenses where they would give out a check and then receive the receipts after reimbursing the employee. This procedure was a control weakness that opened the organization up to fraud. After learning that reimbursements can be faked, they moved to issuing credit cards to their employees for making purchases. In the past the organization only had five credit cards that all employees “shared” to make purchases. The totals for these credit cards fed into the accounting software, but only as totals, and not as individual transactions. This prevented a level of transparency in the accounting software for purchases that were being made. Now each employee receives a card, and every transaction that each employee makes is uploaded into the software. Every transaction now includes the employee’s name that made the purchase. This has helped to reduce fraudulent transactions that can occur. In addition, when a purchase is made by an employee, he or she must take a picture of the receipt and upload it using an App or his or her computer (R9). After scanning the receipt, the employee will have to add other information such as the category account code.

Every employee that receives a card is given a policy on how to use the card appropriately (R10). This credit card procedure helps provide assurance that the transaction that is recorded is not fictitious. In addition, each new card that is issued has specific limits. If an employee reaches the limit that employee’s Delegation of Authority (DOA) is notified. Approval is needed to exceed the limits that are set. This procedure has helped the organization track and view all expenses. There are also controls on the credit cards that prevent the use for activities such as gambling, politics, and others. In addition, meals and travel transactions require permission for processing. One director stated that since the implementation of the employee credit cards procedure credit card usage has dropped by about $100,000 to $150,000 per year (R10). Although the credit card process does add several controls to the organization, it does not prevent every type of fraud. One employee stated that an employee could use the credit card and say, “this is church expenses and be buying personal expenses” (R7).

The organization also has a process for check requests. In the past one employee would enter every check request into the system for processing (R7). Now each department enters their own invoices for payment. There are also controls in place to prevent others from entering invoices in the system. The accounts payable employee is also not able to initiate an invoice. Only the department responsible for the invoice can initiate the process.

Those invoices then go “through a level of authorizations depending on the amount of the invoice and the department” (R7). The first level of approval is the employee’s Delegation of Authority (DOA). The director then has final approval before the requests are sent for processing. After the checks are issued, they must be approved again before the bank will release payment. This provides several layers of approval for every transaction.

Almost all cash transactions are prohibited under the organization’s new policies and procedures. There are minor exceptions for kids’ meals at camp, but the majority of transactions are only credit card or checks (R10). Cash advances are no longer allowed by the organization, and all transactions are now entered into the system electronically. “We don’t have any hard copies anymore” (R10). All hard copies are converted to electronic format for increased ease of review and approval. “Everything is attached to the entry in the accounts payable system” (R10). This allows a manager to review all of the documentation prior to approval. There are different approval structures depending on the amount, such as up to $300, then up to $500 then up to $2,000, and then up to $150,000.

There is also a process used to add new vendors to the system. Since the fraud perpetrated against the organization involved fake vendors, a new process was implemented

(R9). Now the organization must have the vendor's W-9 on file before a vendor can be added. In addition, new vendors must be approved by two employees before being entered into the system. Furthermore, there is a procedure for wire transfers that must be followed. An employee in the business office will call a person associated with the transaction to verify the routing number, account number and other details before the transaction can be executed. Furthermore, if the vendor is a foreign entity the organization is searched against a terrorist watch database, and the vendor will be contacted prior to being added to the system.

In addition to having policies and procedures for the purchasing process, the organizations studied have policies and procedures for their collection process (R1, R4, R5, and R6). One organization stated that this process begins with a department that is responsible for fundraising, acquiring grants, and interacting with contributor and foundations (R1). This department uses software to record income gifts, grants, and other types of funding. The accounting department receives this information through a bridge with their software, where it is then reviewed and accepted. The accounting department then receives the money and deposits it in the bank if it is a check. The employee responsible for deposits said, "I deposit in the bank and then I give the information, like the copy of the check and all the background paperwork that came with it" (R4). After she open the mail she said, "I enter everything on a spreadsheet, so we know how much donations were that day…and any miscellaneous deposits" (R4). After the cash has been deposited another employee stated that, "then I receive them in our system to post to the General Ledger (GL)…and when she's done with the deposit I receive the deposit and I enter in our system" (R5).

One of the organizations that was studied has adopted the philosophy of using a more digital approach to their accounting processes (R8 and R10). They transitioned their check verification, credit card expense procedures, and approval process to an online format. "We eliminate some of the possibility of fraud [with regard] to signatures. So, moving things to an online system as part of that strategy," stated the director (R8). Another benefit of the digital format is the ability to drill down all the way down to the transaction level. This is "so anybody can look at any transaction and see what it is" (R10).

This organization's collection process has changed over the past two years. "Since COVID about 80% of our gifts come online" (R6). For those that are given in person the organization has moved to collection boxes instead of passing a plate. Two people and a security officer are needed to collect the donations in the collection boxes. The finance team does not have access to the items in the drop safe. A security guard is needed to access the donations. A team is then used to count the donations, and then two keys are used to lock the money. The cash is locked in a bank bag and placed in a drop safe. The checks are processed on Mondays in a specific room with a police officer and two or three finance staff. Then an outside security firm is used to collect those funds and deposit them in the bank. Those that are responsible for doing the money counts are not the same employees that are entering the contributions. There are also cameras that record the employees as they count the deposits and two people have to sign off on the deposit amounts.

Access Rights. One of the major types of policies and procedures that are in place are those that are related to access rights. This type of control can take on several forms, but one example is password protection of accounting related software. Several employees mentioned that the accounting software is password protected (R4 and R5). One employee stated, "yes, we have passwords…we're not allowed to give our password out to anyone" (R5).

In addition to password protection, another internal control related to access rights is access related to the accounting software itself. One employee mentioned that, “only the business office has access to the software” (R4). Those that are not in the business office are not granted access to the software. This control prevents those who are not involved in the accounting department from entering or manipulation the financial data.

Every individual in the business office at one organization is given a unique ID. “It’s a penalty of being fired if you share your login ID with someone else” stated one manager (R8). This allows management to track the activity of each employee in the accounting software.

Furthermore, an additional type of access rights is when an organization limits what an employee can access within a process. One of the employees in the business office stated that, “you don’t have access to the whole procedure” (R2). For example, if an employee is responsible for accounts payable, that employee may only be given access to the accounts payable module in the accounting software. This prevents the accounts payable clerk from accessing the payroll module and making fraudulent alterations to the financials.

Software Controls. In addition to having access controls in accounting software, there are other internal controls that have been implemented through an organizations policies and procedures. One example of this is the use of internal controls that are built into the accounting software. One accounting employee stated, “if you put something in, you can’t erase it, I mean, you’ve got a debit and credit always, no matter how many corrections that I make…it’s going to show a trail” (R3). The audit trail that is built into the accounting software is a control that prevents employees from deleting a previously entered transaction. “It’s not like you could put something in and totally delete out where nobody could ever see it,” explained the employee (R3). There is a permanent record even if a transaction is altered or deleted.

Another organization stated that their accounting software is password protected and that there can also be two layers of passwords (R7). In addition, each user has limited access. Users can only see the department they are allowed to bill to. This prevents a user from altering transactions in another department. Another employee reiterated this by saying, "we have it limited by each person's department" through the use of smart roles which will not allow people from other departments to make changes to a department they are not in (R9).

The organization stated that there are a couple employees that have administrative rights for the accounting software (R10). However, for those that do there is a layer of internal controls for the administrators. For example, the director stated, "you cannot change a user's roles and permissions without it notifying someone…There's a group of people that get notified when the roles are changed and permissions are changed" (R10). This protect the organization from having an administrator override the software's internal controls.

The controller at one organization also expressed the desire to move to the cloud version of the financial software (R1). He stated that this version has better internal controls functions, which will lead to more enhancements for the accounting department. The controller is hoping to have this updated software and the controls that it will provide ready in a month after the interview was conducted.

Whistleblower Policy. One of the organizations studied disclosed that they do have a whistleblower policy. One employee stated that they know that they can just go to their boss if they want to report something (R7). Another employee stated that the policy is distributed "as part of the annual performance review process. So, people are aware of the policy" (R8).

The policy allows employees to report any suspected fraud to the Chair of the Finance Committee, who is a non-staff member of the organization (R8). This person will keep reporting of fraud private. An employee stressed that “you’ve got to have an environment where people feel safe reporting things” (R8). Creating this safe environment can be part of the culture that the organization develops for its employees.

Culture. Another area related to policies and procedures was the culture that was developed in the organization. This culture can affect the environment and atmosphere for fraud to occur. One employee stated “Culture is a huge aspect. Making people feel safe [reporting fraud]” (R8). Employees should be safe that they can report fraud anonymously or in a way that does not jeopardize their job or reputation within the organization.

Other Controls. Another policies and procedures control that one of the organizations implemented was having job descriptions. The controller stated that, “we have job descriptions and processes and procedures written. So, the accounting staff understands what their role and function is…to use in doing their work” (R1). Having written job descriptions helps employees understand what their job is within the accounting department. The director of finance in one organization stated that they have a conflict of interest policy that employee must abide to (R10). This prevents employees from making business transactions that benefit the employees through a third party at a cost to the nonprofit organization.

Interpretation of Themes

The themes that were discovered can help other nonprofit organizations detect and deter fraud. Acknowledging that fraud is possible within an organization appears to be the first step in preventing fraud. Avoiding the temptation to trust employees instead of using internal controls is also an important lesson that faith-based nonprofit organizations should follow.

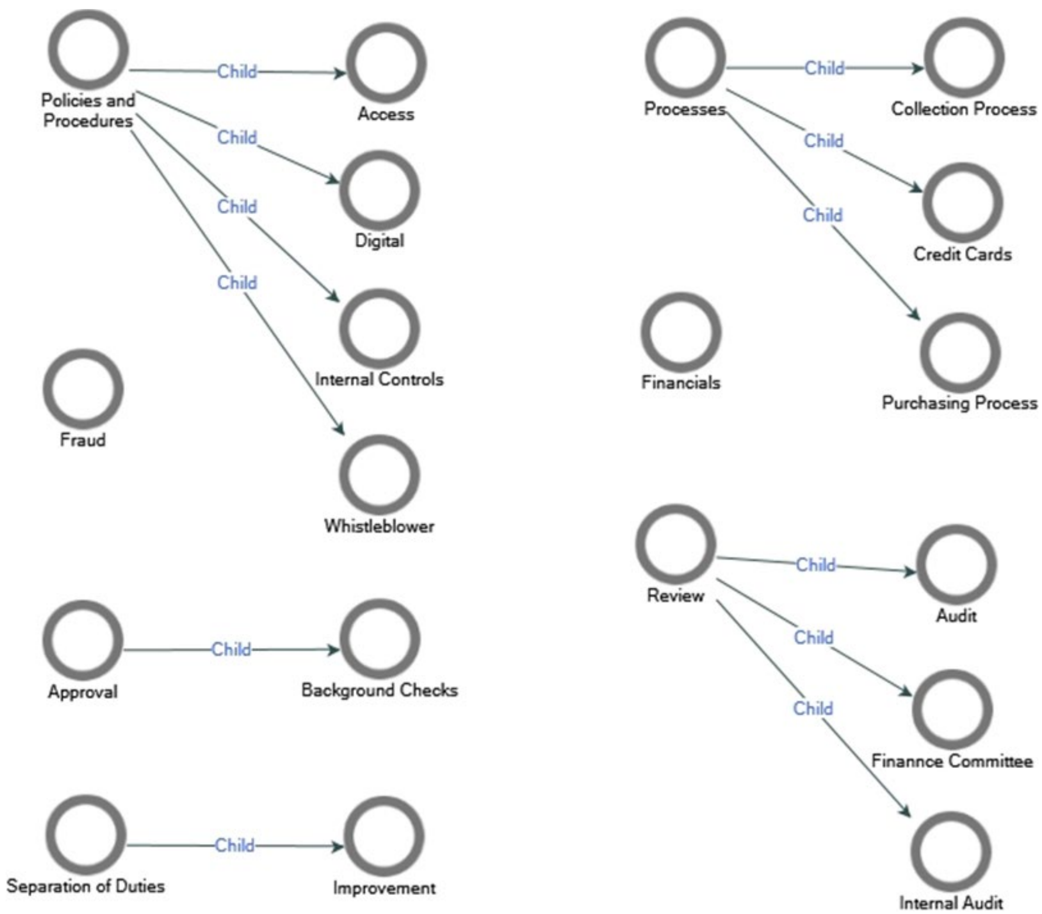
In addition, putting internal controls in place was the best defense to protect an organization against fraud. The test to determine if internal controls are working is to see if major fraud has occurred with the internal controls in place. Nonprofit organizations report major fraud that was discovered on their annual Form 990 that they file with the Internal Revenue Service (IRS). The Form 990s for one of the organizations was reviewed for the most recent three years available as of the time of the study. Part VI question 5 on the Form 990 addresses issues related to fraud. The question asks, “Did the organization become aware during the year of a significant diversion of the organization’s assets?” This question was designed to disclosure significant frauds that the organization discovers. For all three years the organization answered “no” to this question, which means that they did not discover a large fraud within the organization. This could be the result of having internal controls in place to decrease the opportunity to commit fraud.

Representation and Visualization of the Data

The findings can be represented with visualizations in several regards. The first visualization of the data was related to the coding that was used for the findings. The coding that was developed was based on the major themes that were discovered throughout the fieldwork. Each major theme and some minor themes were each given a code. Figure 4 depicts the parent and child level codes that were created for the study. The parent level codes are approval, financials, fraud, policies and procedures, processes, review, and separation of duties. Some of the parent level coding categories were further divided with child level coding categories. For example, the policies and procedures parent level code has four child level coding categories, which are: access, digital, internal controls, and whistleblower. The child level codes contain data that is related to the parent level code. Some of the parent level codes did not fit into any of the child level codes and were only coded with the parent level code. In addition to policies and procedures, the process code has three child level codes which are collection process, credit cards, and purchasing process. The review code has three child codes which are audit, finance committee, and internal audit. The separation of duties' child code is improvement and the approval child code is background checks.

Figure 4

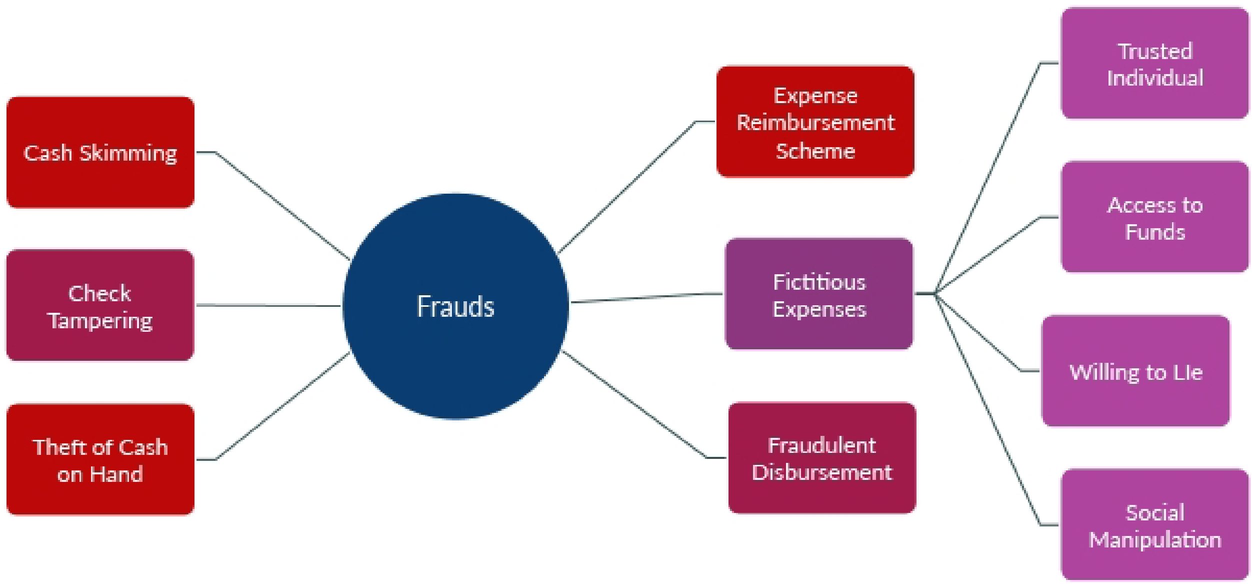
Coding Map



The second visualization of the data is related to the frauds that were discovered during the fieldwork. There were six frauds that were shared by the organizations that were studied as depicted in Figure 5. These frauds were cash skimming, check tampering, theft of cash on hand, expense reimbursement scheme, fictitious expenses, and fraudulent disbursement. The major fraud that was studied was the fictitious expenses fraud. This fraud was primarily fraudulent receipts but did include other fraud types by the perpetrator. The organization shared four factors that exposed the organization to the large fraud (R6). These four factors are trusted individual, access to funds, willingness to lie, and social manipulation.

Figure 5

Frauds Studied



Relationship of the Findings

The findings that were discovered through this study are related to many of the topics discussed earlier in the study. The relationship of the findings will be discussed with respect to the research questions, the conceptual framework, the anticipated themes, the literature, and the problem. Each of these sections that were discussed earlier will be compared to the findings that were discovered through the fieldwork.

The Research Questions. The finding from the research are related to each of the three research questions discussed earlier. The first research question (RQ1) was: what are the factors that can lead to increased risk of fraud, the waste of funds, or the abuse of funds within faith-based nonprofit organizations? The factors related to the findings are the several instances of fraud discovered from the interviews. One employee stated that there are four factors that can lead to an increased risk of fraud, the waste of fund, or the abuse of funds within an organization (R6). These four factors are a trusted individual, access to funds, a willingness to lie, and social manipulation. In addition, other employees stated that a lack of manager supervision can lead to an opportunity for fraud to go undetected (R8 and R10).

The findings were also related to the second research question (RQ2), which was: what are the strategies and internal controls that faith-based nonprofits can implement to mitigate the risk of fraud, the waste of funds, or the abuse of funds? The findings from the research that are related to this research question are each of the identified themes that were discovered. These themes are segregation of duties, approval controls, review process, and policies and procedures. Each of these themes contain both strategies and internal controls that can help to mitigate the risk of fraud, the waste of funds, or the abuse of funds. After discovering fraud in one organization the leadership implemented many new controls and processes. "We've closed the loopholes that we know about...I think we feel like it's effective because we know we've closed the loopholes" (R8).

The third research question was: what are the strategies and internal controls that faith-based nonprofits in Texas can implement to mitigate the risk of fraud, the waste of funds, or the abuse of funds? This question was related to organizations specifically located in Texas. Each of the organizations studied are located in Texas. All of the findings from the research are related to internal controls of faith-based organizations in Texas. These organizations have real property in Texas and have employees living and working in Texas. The strategies and internal controls that were found were obtained from Texas organizations.

The Conceptual Framework. The conceptual framework discussed in this study was the fraud triangle. This theory states that there are three components that fraud includes three key elements, which are pressure, rationalization, and opportunity (Kelly, 2017). The opportunity element is the element that is focused on in this study since it is the one that organizations have the most control over.

In the interviews that were conducted one organization stated that they found that an employee was stealing funds from the tip jar in the restaurant (R1). This employee was able to commit fraud because he had the opportunity to do so. He had access to the money and was able to take it when other employees were not watching. This employee was caught and was confronted by management. This correlated to the conceptual framework which theorizes that people will commit fraud if they have pressure, rationalization, and opportunity. Although organizations may not know what pressures employees have outside of their organizations or the rationalization that they use to justify committing a fraud, they can control the opportunity. Putting internal controls in place can help to reduce the opportunity. In this case an internal control could be supervision. The tip jar could be placed next to the cash register, and the employee that oversees the register could be responsible for overseeing the tip jar. In addition, a camera could be installed that records the transactions that take place at the register as well as the tips that are received from the customers.

Another example of attempted fraud was discovered by the accounting department at one of the organizations that was interviewed. As discussed earlier one organization uses an internal control for their check disbursement process (R3). This control involves approving all check disbursements prior to processing by the bank. No check can be cashed unless it is approved by an employee in the organization. This type of controls has prevented several attempts to process a fraudulent check. These fraud attempts were able to be thwarted because the opportunity to commit fraud was removed.

Anticipated Themes. Prior to conducting the fieldwork aspect of the study there were several themes that the researcher anticipated. It was anticipated that the nonprofit organizations would have some internal controls in place as part of their normal policies and procedures. The anticipated internal controls would include controls related to segregation of duties, controls related to approval, and controls related to access. The extent of these controls was expected to be lower than those in the corporate environment. It was also anticipated that the organizations would have some level of background checks, a whistleblower policy, and possibly a conflict of interest policy. Furthermore, the researcher anticipated not seeing the use of an audit committee due to the size of the nonprofit organizations that were studied.

There were several minor themes that were discovered that were not anticipated by the researcher. The use of financial analysis such as trend analysis was used by one of the organizations that was researched that was not anticipated as a theme (R8). The use of internal auditors was also not anticipated, however one of the organizations studied had employed an internal audit firm (R6). It was also not anticipated that the tone at the top culture would have an impact on the occurrence of fraud, however this was the case in one of the organizations that were studied (R6). In addition, the extent of prior fraud occurrences was not anticipated by the researcher (R1 and R6). All of the organizations that were studied had some occurrences of fraud. One of those occurrences were very large, but most of them were relatively minor.

The Literature. The findings from this study are also related to the literature in several aspects. The literature states that asset misappropriation represent over 95% of frauds committed in nonprofit organizations (Greenlee et al., 2007). This statistic is representative of the frauds that were disclosed in the findings. Six frauds were shared with the researcher and all six involved misappropriations of the organization's assets (both cash and other assets), which is 100% of the frauds studied.

The literature also states that nonprofits are oftentimes susceptible to fraud because they have a high level of trust of their employee (Soobaroyen & Sannassee, 2007). This was also the case in the major fraud that was shared in the findings. One of the employees said that there were four factors that contributed to the fraud with the first factor being that the fraudster was a trusted employee. This level of trust allowed the fraud to continue longer than it would have if it was an untrusted employee.

The likelihood of survival after a major fraud was also discussed in the literature. Archambeault and Webber (2018) studied the survival rates of nonprofits that survived a major fraud and found that one four of them do not survive after three years of a fraud being made public. The organization from the findings that experienced a major fraud had survived longer than the three-year mark that was used in the literature. The organization in the findings was in its fourth year after going public with the fraud and they were still operating the organization. The literature further found that older and larger organizations were more likely to survive a fraud than younger and smaller ones (Archambeault & Webber, 2018). The organization in the findings was both larger and older than the average nonprofit organization. Incidentally, the organization in the findings was so old that it has a Texas historical marker on its premise to highlight the historical significance of the organization.

The literature also states that there are two control practices that are performed less frequently by those organizations that have experienced fraud than those who have not. One of those practices was the review of expenses (Snyder et al., 2017). In the findings the organization that experienced the major fraud disclosed that the fraudster was not being adequately reviewed for his credit card charges. There were no limits in place for this individual and there was not proper approval and testing of the individual's expenses. Had there been a higher level of review of the fraudster's expenses the fraud may have been detected much earlier. Snyder et al. (2017) further stated that organizations that did experience major fraud made several changes to their internal controls. This was also the case for the organization in the findings that discovered majored fraud. They hired an internal audit firm to evaluate every accounting process in the organization and did a risk assessment to find ways to improve all of the internal controls (R6). In addition, the organization hired a fraud investigator to determine how the fraud occurred and to find ways to prevent future frauds from occurring. As a result, the organization changed many of their policies and procedures, including eliminating employee reimbursements and using individual credit cards to track the purchases made by each employee.

Greenlee et al. (2007) found that larger fraud was associated with collusion, higher salaries, age, educational level, and longer tenure with the organization. In the major fraud from the findings the fraudster was an employee that had a long tenure in the organization (R8). He had worked for that organization for seventeen years, and likely would have been a member of the church for even longer than that. The median tenure for employees that committed fraud from the literature was seven years, so this employee was considered a long-term employee from the literature standards (Greenlee et al., 2007). The most common type of fraud from the literature was fraudulent disbursements, which was paying for an expense that the company does not owe (Greenlee et al., 2007). This was the same type of fraud that was committed by the fraudster in the findings.

The literature also states that 72% of the cases led to the termination of the employee and those who had committed large frauds were criminally prosecuted 72% of the time (Greenlee et al., 2007). The major fraud from the findings aligned with the literature. The fraudster was terminated from his position at the organization, was prosecuted, and found guilty (R10).

The Problem. The findings are also related to the problem statement discussed at the beginning of the study. The general problem to be addressed was the lack of strategies and internal controls in nonprofit organizations resulting in a higher risk of fraud in charities, churches, and government entities. The findings confirmed that there was a higher risk of fraud in nonprofit organizations due to the smaller size and limited resources that nonprofits have as compared with for-profit corporations. One organization that was interviewed stated that due to the limited number of people in the accounting department there are challenges in ensuring that all duties are fully separated (R1). The organization stated that the critical functions are separate, but there is some crossover in other functions, which is compensated using various levels of review. Another organization that was interviewed also stated that limited staff can be an issue (R8).

The specific problem statement to be addressed was the lack of internal controls in faith-based nonprofit organizations within Texas resulting in a higher risk of fraud within those entities. This specific problem statement was related to the findings in that all of the organizations that were researched were faith-based nonprofit organizations that are located in Texas. Each of the themes that were discovered are applicable to this population. None of the organizations that were studied were entities outside of Texas, and therefore each of the findings are directly related to the specific problem statement.

Summary of the Findings

In summary, this section discussed several areas related to the findings of the study. The major theme that were discovered are frauds occur, segregation of duties, approval controls, review process, and policies and procedures. The frauds occur theme showed that frauds do occur in faith-based nonprofit organizations, even when employees do not expect to find it. The segregation of duties theme demonstrated that one employee should not be responsible for all of the duties in the accounting department, and that practices such as employee rotation can help in areas where segregation of duties was not possible. The approval controls theme uncovered the need for management approval of accounting tasks and should include background checks of new employees. The findings also identified the review process theme, which states that a third party should review the work of the accounting department whether that be through an external audit, an internal audit, or other types of internal review. The last theme that was discovered was policies and procedures which uncovered that organizations need to have a process in place for collecting revenue and for making purchases. These policies and procedures should also cover access rights to the accounting software, a whistleblower policy to anonymously report fraud, and policies that develop a strong ethical culture in the organization. These themes were interpreted to be consistent with the literature. Faith-based nonprofit organizations are susceptible to fraud, however strong internal controls and other strategies can help mitigate the risk of fraud.

The findings that were discovered were summarized in two data visualizations. The first visualization depicted the major and minor themes that were discovered. The second visualization showed the types of fraud that were uncovered during the fieldwork. The findings are related to the research questions in that several instances of fraud were shared by the interviewees as well as several strategies and internal controls that the organizations use to detect and deter fraud. The conceptual framework also relates to the findings through the opportunity aspect of the fraud triangle, which theorizes that if there is an opportunity to commit fraud some employees will attempt to exploit that opportunity.

Several of the themes that were discovered were anticipated prior to the fieldwork, however the use of financial analysis, internal auditors, and the number of frauds discussed was not anticipated. The findings were also consistent with the literature in that most fraud was related to asset misappropriation, and due to a high level of trust by the organization. The literature was also consistent with the findings regarding organizational survival of major fraud, and the termination and prosecution of major fraud. The findings also reinforced with the problem statement that there was a lack of strategies and internal controls in faith-based organizations. This deficiency has led to several frauds that were discovered. One employee rightly summarized the findings by saying, “I think the thing to hammer home would be don’t be naïve enough to think it’s not going to happen in your organization. It’s probably just a question of how much and to what degree” (R8).

Table 2

List of Participants

Name	Description
Respondent 1 (R1)	Position is controller and oversees the operations of the accounting group, budgeting, and special projects.
Respondent 2 (R2)	Senior accountant responsible for the bank reconciliations, fixed assets, and extraordinary expenses.

Respondent 3 (R3)	Accounts payable clerk responsible for making payments.
Respondent 4 (R4)	Accounts receivable clerk responsible for revenue and deposits.
Respondent 5 (R5)	Assistant accounts receivable responsible for deposits and customer data.
Respondent 6 (R6)	Executive pastor that oversees the operations, human resources, and finances of the organization.
Respondent 7 (R7)	Financial assistant and accounts payable clerk for checks and credit cards.
Respondent 8 (R8)	Director of Operations and oversees financials, facilities, information technology, and security.
Respondent 9 (R9)	Financial services associate responsible for contributions.
Respondent 10 (R10)	Director of Finance which oversees finances, monthly reporting, and budgeting.

Application to Professional Practice

This study can provide several applications to the professional practice. It can help to improve general business practices in the field of accounting in faith-based nonprofit organizations. In addition, this study can provide potential application strategies based on the findings that can help all nonprofit organizations.

Improving General Business Practice

The research from this study can be used to improve general business practices. The first way this study can improve general business practices is by helping nonprofits adopt a culture of good accounting practices. Management should emphasize the importance of following internal control practices and invest the time and resources to create a culture that follows these policies. Management should not rely on trusted employees as their anti-fraud strategy. “He wasn’t under the same scrutiny as everybody else,” responded one employee regarding a fraudster who was able to perpetrate a major fraud for 10 years. Many frauds occur because management relied on trust instead of implementing internal controls. In addition, every employee should be expected to follow the organizations policies and procedures. Requiring all employees to follow the organization’s policies and procedures will help to improve general business practices.

General business practices can also be improved when nonprofits accept that fraud can happen to them. Many nonprofits believe that no one at their organization would commit a fraud. An employee at one of the organizations that was studied stated, “I was wildly naive. I would have told you there was no way in a million year somebody could take a million dollars from our church and I would have believed it to the core of my being.” This level of naivety prevents these organizations from seeing the need for internal controls. Policies and procedures are ignored because managers do not see the need for them. This study has shown that major fraud can occur at organizations that think they are immune to fraud.

Organizations can also learn how to look for red flags and to report them when they see them. In this study a major fraud was committed against an organization and it was not detected for many years, even though there were some red flags. One employee admitted, “we ignored red flags, so pay attention to the flags in general and listen to the people when they make them.”

These flags were not directly related to the fraud; however, they were related to the individual's character and could have been investigated. Reporting red flags can help to improve the general business practices in nonprofit organizations.

This study has also shown that when internal controls are put in place, they provide a higher level of transparency and accountability for the organization. These two qualities are what one employee felt were the greatest attributes for detecting and preventing future frauds. By involving more of the organization in the review process of the financials there was less opportunity for fraud to hide. This general business practice allows more eyes to see the financials and review them for accuracy. Accountability is also a general business practice that can improve through this study. Holding managers accountable for their department and holding employees accountable for their purchases, organizations are able to make their employees more accountable for the financial transactions of the organization.

Improvement in general business practices is desperately needed in faith-based nonprofit organizations to help curb the rate of fraud that is occurring. One employee reminded nonprofits that, "you know, it's happening in every nonprofit. It's just a matter of how much, and is it getting caught" (R8)? Good business practices are crucial to detecting and deterring fraud. It helps the organization become aware of potential fraud within the organization. One participant in the study shared, "one of the interesting things about fraud is it can go right by you if you're not aware" (R8). Being aware of fraud is needed to be able to stop it because the reality of fraud is that "it happens unfortunately" (R8). Knowing that fraud is occurring in nonprofit organizations is the first step in combatting it. One employee summarized that the next step is that "[we] got to figure out a way to catch them" (R6). Having good general business practices is a major step in the direction of making faith-based nonprofits more protected from the attack of fraud.

Potential Application Strategies

There are several potential application strategies that nonprofit organization can implement to mitigate the risk of fraud. One strategy is a whistleblower policy. All nonprofit organizations should have a whistleblower policy in place. Tips received from whistleblowers are the single most effective fraud detection method, with 40% of occupational fraud in nonprofits being detected through this method (ACFE, 2020). Half of the tips received are from employees, so providing this procedure for an organization is crucial. Employees who report suspicious activity should be able to do so anonymously if they chose through a fraud hotline or other means. This tool is one of the most important fraud prevention strategies that an organization can implement. This service can even be outsourced to a third party for added confidentiality for a relatively low cost.

Another strategy is to have some type of review of the financial statements, policies, and procedures. This can take the form of hiring external and internal auditors, but this strategy can help deter fraud. Twelve percent of all frauds are detected by external auditors and 17% are detected by internal auditors (Greenlee et al., 2007). Even though an external auditor is technically not hired to find fraud, their presence at the organization will help to deter fraud. The perception that the auditors will review documentation is enough to deter some employees from committing fraud. In addition, an audit can help review management. Since 60% of frauds are committed by executive management it is important to review those who have the most authority (Greenlee et al., 2007).

In addition to review strategies, organizations should perform background checks on their employees prior to hiring them. This is a low-cost strategy that can help an organization discover red flags about an employee's character before he or she is hired. Several multimillion-dollar frauds have occurred because the organization failed to conduct a background check prior to hiring the employee (Gallagher & Radcliffe, 2002). These background checks can include checking references, education, credit history, and criminal history (Murphy, 2015).

Organizations should have proper policies and procedures in place. One of those policies should include establishing job descriptions that allow for segregation of duties among the staff. Allowing an employee access to both the assets and accounting records creates a large opportunity for fraud. This would allow an employee to steal an asset and then cover up the theft by altering the accounting records. Therefore, proper segregation of duties is necessary.

Dividing a process between two or more employees is one way to segregate duties. For example, if one employee is responsible for collecting cash, another should be responsible for recording the deposits in the accounting system and a third could be responsible for the bank reconciliation. This prevents one employee from having too much access to the assets and accounting records.

Some organizations are too small to fully utilize segregation of duties. In these cases, supervision should be used to compensate for a lack of segregation of duties. For instance, if one employee is counting cash and recording the deposit, a supervisor should review the cash count and deposit before recording the transaction. Organizations can also have employees rotate duties to keep one employee from concealing a fraud. Many frauds must be held together to maintain concealment, and employee rotation or mandatory vacations is one way to uncover these schemes.

In addition to segregation of duties, access to processes and procedures should be limited. Accounting staff should have limited access to the accounting software. The accounts payable clerk should not have access to fixed assets, accounts receivable, and the general ledger. Access should only be given to employees for functions that they must have to do their job.

Summary of Application to Professional Practice

The research from this study can help improve general business practices. It can help create a culture of good accounting practices, help organization to not be naïve about fraud, and to help them to pay attention to red flags. The study can also help increase transparency and accountability which is needed to detect and deter fraud. The research can also help faith-based nonprofit organizations develop potential application strategies such as a whistleblower policy, an annual audit, performing background checks, and creating segregation of duties.

Recommendations for Further Study

Based on the findings of this study there are several areas that should be studied further. One recommendation is to conduct research to determine if the risk of fraud is reduced when a large proportion of giving is processed electronically instead of through cash donations. This study could help nonprofit organizations evaluate if there is a benefit to accepting electronic donations in the form of reduced risk of fraud against the organization. Another related area for further study is to determine if the additional cost of processing online donations exceeds the risk of fraud from cash donations. Since there is a cost to process credit and debit card transactions for the organization, this cost can be compared to average cost of fraud for a nonprofit organization to determine if the benefits exceed the costs.

Another area for further study is to understand the aftereffects of a faith-based nonprofit organization that has experienced major fraud that has been made public. One aspect could be to see if the implementation of internal controls after a major fraud can help to restore donor trust and prevent the organization from losing contributions in the future. Another area of research that is needed is to determine the effect a publicized fraud has on church attendance and donations. Determining if there is a correlation between the two could be an area for further research. Since this study involved the discovery of a major fraud in a church, further research to understand its effects could be an area of further study.

Reflections

The reflections section will discuss personal and professional growth that has occurred from conducting this study. It will be followed by a Biblical perspective that can be viewed in relation to this research. These reflections have provided added benefits to the efforts of conducting this study.

Personal and Professional Growth

Conducting this study has provided both personal and professional growth in several areas. This research has provided professional benefit through learning more about internal controls as they relate to nonprofit organizations. It has provided opportunities to meet with accountants in the field to learn which controls are being used in practice versus those that are discussed in the classroom. This study has also helped to connect theory with practice in this area of internal controls.

In addition, this study has helped the researcher learn the process for studying a topic and publishing the findings. This area of professional growth can be of benefit in the future in the realm of post-doctorate research, which is an area of interest to the researcher. The researcher has also enjoyed the journey of conducting research on a topic, compiling that data, and assimilating it into a report or publication. This growth has provided the foundation to continue research in the area of accounting, as well as other fields of study that are of interest. The researcher hopes to be able to use these techniques to write several articles for accounting journals.

This study has also benefited the researcher on a personal level. Having worked at two faith-based nonprofit organizations, he has witnessed the use of internal controls, or lack thereof, and have always wanted to find ways to improve those controls so that these organizations are better protected against fraud. This study has helped him to learn how to better equip those organizations if he decides to work in the finance department at another faith-based nonprofit organization.

The researcher also has a personal interest in seeing faith-based nonprofit organizations have better internal controls so that the organizations can focus on their mission, which is to serve the community in the name of Jesus. When these organizations are able to lower the risk of fraud, they can spend more time carrying out the vision of the organization. Less time will be wasted on prosecuting frauds committed against the organization, and more time can be spent on the purpose of the organization.

Biblical Perspective

The business functions explored in this study were primarily internal controls and strategies used to decrease the risk of fraud within nonprofit organizations. Internal controls integrate with a Christian worldview in that internal controls are attempting to prevent fraud and errors from occurring in an organization. Without internal controls the opportunity to commit fraud and deceive an organization would be too great. Proverbs 20:17 (ESV) says, “Bread gained by deceit is sweet to a man, but afterward his mouth will be full of gravel.” This scripture shows that fraud is attractive to people in that they are gaining something that they did not have to work for. However, once they are caught, which can occur through the use of strategies and internal controls, that sweetness is turned into something distasteful (e.g., gravel). The ultimate payoff of fraud is jail, fines, and severe damage to one's reputation.

Jesus also taught on the importance of honesty both in the workplace and in general. He said, "one who is faithful in a very little is also faithful in much, and one who is dishonest in a very little is also dishonest in much." Luke 16:10-11 ESV. Those who are willing to cheat in small ways will also cheat in large ways if given the opportunity. That is why policies and procedures are very important in an organization. For example, if an organization does background checks on their employees, they might discover that a potential employee has a criminal history of theft. Entrusting this employee with the organization's finances could put the organization at risk for fraud.

Individuals that do commit fraud tend to use their ill-gotten gain for lavish lifestyles instead of building up a savings and investing in the future. Proverbs 10:2 (ESV) echoes this sentiment by stating, "Treasures gained by wickedness do not profit, but righteousness delivers from death." Most fraudsters waste the money they have stolen, and the end result is that they are just as broke after the fraud is discovered as they were before they committed the fraud.

Jesus also stressed the importance of one's soul over money. He said, "For what does it profit a man to gain the whole world and forfeit his soul?" Jesus was teaching that one's soul is worth more than all of the riches this world has to offer. However, he also is showing that riches are nothing compared to eternal life in Christ. Seeking after money, while ignoring one's spiritual development is pointless. That is why committing fraud is really a fruitless endeavor. It may enrich one's life, but that enrichment is only temporary, and does not lead to lasting fulfillment.

Fraud is often committed out of a love for money, and a desire to have more, even at the expense of others. 1 Timothy 6:9-10 (ESV) says, "But those who desire to be rich fall into temptation, into a snare, into many senseless and harmful desires that plunge people into ruin and destruction. For the love of money is a root of all kinds of evils." This love for money has caused some people to set aside morality and sensibility to take something that does not belong to them in order to feed the greed for more money.

Some people that commit fraud against their employer will justify to themselves that they were eventually going to pay it back. Psalm 37:21 (ESV) states that, "the wicked borrows but does not pay back, but the righteous is generous and gives. Those who commit fraud may tell themselves that they are planning to pay the organization back, however this is often just justification to ease their conscience.

The Bible is very clear that committing fraud is a sin, and not something that should be done. One of the Ten Commandments addresses stealing, and Leviticus further iterates, "You shall not steal; you shall not deal falsely; you shall not lie to one another" (Leviticus 19:11 ESV). All fraud involves stealing and oftentimes lying to be accomplished. Therefore, it is clearly against God's commands to commit fraud. That is why adding internal controls and strategies is Biblical and necessary to protect an organization's finances.

All of the internal controls discussed in this study are designed to promote honesty in the workplace. These controls lower the opportunity and thus lower the temptation to commit fraud. By removing the opportunity to commit fraud, an organization is more likely to accurately convey their financial health to those parties that rely on the financials for decision making.

Summary of Reflections

Reflecting back on this research study has resulted in several benefits that have significantly impacted my life. This study has led to both personal and professional growth and has left many experiences by which I have grown from. In addition, this research has helped me to see how internal controls in accounting have applications to Biblical principles. These reflections have left a lasting impact on my life that I will remember for years to come.

Summary of Section 3

Section 3 discussed the overview of the study, the presentation of the findings, the application to professional practice, recommendations for further study and reflections. The presentation of findings included the themes that were discovered and the interpretation of the themes, the visualization of the data, and the relationship of the findings. The application to professional practice discussed how this study can improve general business practices as well as potential application strategies. Section 3 concluded with personal and professional growth reflections as well as Biblical perspective reflections.

Summary and Study Conclusions

In conclusion, this study addressed the problem that there are a lack of strategies and internal controls in faith-based nonprofit organizations resulting in a higher risk of fraud, waste of funds, or abuse of funds in these organizations. Lack of resources and the trust of these organizations in their employees was the cause of some of this increased risk. This qualitative case study researched two faith-based nonprofit organizations in Texas and found several themes that emerged. These themes are segregation of duties, review process, frauds occur, approval controls, and policies and procedures. Policies and procedures that these organizations used to mitigate the risk of fraud included background checks, whistleblower policies, segregation of duties, review of financials, and limited access. Although the risk of fraud can never be fully eliminated, these policies and procedures can help reduce the risk, and allow faith-based nonprofit organizations to carry out their mission over serving others and sharing their faith.

References

Abdullahi, R., & Mansor, N. (2018). Fraud prevention initiatives in the Nigerian public sector: Understanding the relationship of fraud incidences and the elements of the fraud triangle theory. *Journal of Financial Crime*, *25*, 527–544. http://10.1108/JFC- 02-2015-0008

Abu Khadra, H., & Delen, D. (2020). Nonprofit organization fraud reporting: does governance matter? *International Journal of Accounting and Information Management*, *28*(3), 409–428. https://doi.org/10.1108/IJAIM-10-2019-0117

Abdul Rahman, A. A. A., & Al-Dhaimesh, O. H. A. (2018). The effect of applying COSO-ERM model on reducing fraudulent financial reporting of commercial banks in Jordan. *Banks and Bank Systems*, *13*(2), 107–115. https://doi.org/10.21511/bbs.13(2).2018.09

ACFE. (2020). *The fraud tree*. https://www.acfe.com/rttn2016/images/fraud-tree.jpg

ACFE. (2020). *Report to the nations: 2020 global study on occupational fraud and abuse*. https://www.acfe.com/report-to-the-nations/2020/

Agar, M. H. (1980). *The professional stranger: An informal introduction to ethnography.* Academic Press.

Ahmed, A. M., & Muhammed, A. A. (2018). Internal control systems & its relationships with the financial performance in telecommunication companies - a case study of Asiacell. *International Journal of Scientific and Technology Research*, *7*(11), 82–88. https://doi.org/10.29358/sceco.v0i28.416

Albrecht, C., Holland, D., Malagueño, R., Dolan, S., & Tzafrir, S. (2015). The role of power in financial statement fraud schemes. *Journal of Business Ethics*, *131*, 803–813. https://doi.org/10.1007/s10551-013-2019-1

Albrecht, W. S., Albrecht, C. O., & Albrecht, C. C. (2016). *Fraud examination* (5th ed.). Cengage Learning.

Aldrich, H., & Auster, E. R. (1986). Even dwarfs started small: Liabilities of age and size and their strategic implications. *Research in Organizational Behavior*, *8*, 165–186. https://www.econbiz.de/Record/even-dwarfs-started-small-liabilities-of-age-and-size-and-their-strategic-implications-aldrich-howard/10001042804

Applegate, D. (2019). Assessing and controlling nonprofit fraud risk. *Strategic Finance*, *100*, 35–41. https://sfmagazine.com/past-issues

Archambeault, D. S., & Webber, S. (2018). Fraud survival in nonprofit organizations: Empirical evidence. *Nonprofit Management and Leadership*, *29*(1), 29–46. https://doi.org/10.1002/nml.21313

Archambeault, D. S., Webber, S. J., & Greenlee, J. (2015). Fraud and corruption in U.S. nonprofit entities: A summary of press reports 2008-2011. *Nonprofit and Voluntary Sector Quarterly*, *44*(6), 1194–1224. https://doi.org/10.1177/0899764014555987

Aris, N., Arif, S., Othman, R., & Zain, M. (2015). Fraudulent financial statement detection using statistical techniques: The case of small medium automotive enterprise. *The Journal of Applied Business Research*, *31*, 1469–1475. http://www.cluteinstitute.com

Azmat, M., Atif, M., & Kummer, S. (2019). Identification and prioritization of critical success factors in faith-based and non-faith-based organizations' humanitarian supply chain. *Journal of International Humanitarian Action*, *4*(1), 1–17. https://doi.org/10.1186/s41018-019-0067-6

Baapogmah, F. A., Mayer, R., Chien, W. W., & Afolabi, A. (2015). Control mechanisms and accountability challenges in nonprofit organizations. *Global Journal of Business Research*, *9*(1), 27–38. https://ssrn.com/abstract=2654450

Bakri, H., Mohamed, N., & Said, J. (2017). Mitigating asset misappropriation through integrity and fraud risk elements. *Journal of Financial Crime*, *24*, 242–255. https://doi.org/10.1108/JFC-04-2016-0024

Baron, M. A. (2008). *Division of Educational Administration: University of South Dakota*, *1*, 1–52. https://www.regent.edu/acad/schedu/pdfs/residency/su09/dissertation_guidelines.pdf

Bloomberg, L. D., & Volpe, M. (2012). *Completing your qualitative dissertation: A road map from beginning to end* (2nd ed.). Sage.

Boenigk, S., & Becker, A. (2016). Toward the importance of nonprofit brand equity. *Nonprofit Management and Leadership*, *27*(2), 181–198. https://doi.org/10.1002/nml.21233

Bonny, P., Goode, S., & Lacey, D. (2015). Revisiting employee fraud: Gender, investigation outcomes and offender motivation. *Journal of Financial Crime*, *22*, 447–467. https://doi.org/10.1108/JFC-04-2014-0018

Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, *34*, 578–596. https://doi.org/10.1016/j.jaccpubpol.2015.05.006

Branson, L., Buxton, M., & Canny, M. (2015). The adoption of document retention policy in nonprofit organizations. *International Journal of Business, Accounting and Finance*, *9*, 64–74. http://www.iabpad.com/journals/international- journal-of-business-accounting-finance

Brasel, K. J. (2020). *Survey research* (pp. 237–248). Cham: Springer International Publishing.

https://doi.org/10.1007/978-3-030-28357-5_20

Bunn, E., Ethridge, J., & Crow, K. (2019). Fraud in small businesses: A preliminary study. *Journal of Accounting and Finance*, *19*, 24–32. http://www.na-businesspress.com/jafopen.html

Burks, J. J. (2015). Accounting errors in nonprofit organizations. *Accounting Horizons*, *29*, 341–361. https://doi.org/10.2308/acch-51017

Burt, I. (2016). An understanding of the differences between internal and external auditors in obtaining information about internal control weaknesses. *Journal of Management Accounting Research*, *28*(3), 83–99. https://doi.org/10.2308/jmar-51471

Campbell, S., Li, Y., Yu, J., & Zhang, Z. (2016). The impact of occupational community on the quality of internal control. *Journal of Business Ethics*, *139*(2), 271–285. https://doi.org/10.1007/s10551-015-2624-2

Chan, Z. C. Y., Fung, Y., & Chien, W. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process? *Qualitative Report*, *18*(30), 1. https://doi.org/10.46743/2160-3715/2013.1486

Chen, H., Dong, W., Han, H., & Zhou, N. (2017). A comprehensive and quantitative internal control index: construction, validation, and impact. *Review of Quantitative Finance and Accounting*, *49*(2), 337–377. https://doi.org/10.1007/s11156-016-0593-x

Chen, Q., Salterio, S., & Murphy, P. (2009). Fraud in Canadian nonprofit organizations as seen through the eyes of Canadian newspapers, 1998–2008. *The Philanthropist*, *22*, 24–40. https://smith.queensu.ca/_templates/documents/governance/reports/fraud-in-canadian-nonprofit.pdf

Church Finder. (2021). Christian churches in Houston Texas. *Church Finder.com.*

https://www.churchfinder.com/churches/tx/houston

Connolly, C., & Hyndman, N. S. (2004). Performance reporting: A comparative study of British and Irish charities. *The British Accounting Review*, *36*(2) 127–154. https://doi.org/10.1016/J.BAR.2003.10.004

COSO. (2020). *Executive summary*. https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

COSO. (2017). *Integrated framework principles*. https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

COSO. (2016). *Fraud risk management guide.* Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, *15*(6), 738–743. https://doi.org/10.2307/2086606

Creswell, J. W. (2015). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.

Creswell, J. W., & Báez, J. C. (2020). *30 essential skills for the qualitative researcher*. Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Sage.

Derby, R. (2015). *Financial management in selected charismatic churches in the Kumasi metropolis* [Master's thesis,]. http://www.knust.edu.gh

Dickens, D., & Fay, R. (2017). COSO 2013: Aligning internal controls and principles. *Issues in Accounting Education*, *32*, 117–127. https://doi.org/10.2308/iace-51585

Dimitrijevic, D., Milovanovic, V., & Stancic, V. (2017). The role of a company's internal control system in fraud prevention. *E-Finanse*, *11*(3), 34–44. https://doi.org/10.1515/fiqf-2016-0117

Douglas, S., & Mills, K. (2000, August 16). Nonprofit fraud: What are the key indicators? *Canadian Fundraiser*. http://www.charityvillage.com/cv/research/ rlegal16.html

Duckles, B. M., Hager, M. A., & Galaskiewicz, J. (2005). How nonprofits close: Using narratives to study organizational processes. *In* K. D. Elsbach (Ed.), *Qualitative organizational research: Best papers from the Davis conference on qualitative research* (pp. 169–203). Information Age Publishing.

Ege, M. (2015). Does internal audit function quality deter management misconduct?. *The Accounting Review*, *90*, 495–527. https://doi.org/10.2308/accr-50871

Felix, R., Gaynor, G., Pevzner, M., & Williams, J. L. (2016). Societal trust and the economic behavior of non-profit organizations. *Advances in Accounting*, 1–32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2799466

Fitri, F., Syukur, M., & Justisa, G. (2019). Do the fraud triangle components motivate fraud in Indonesia?. *Australasian Accounting, Business and Finance Journal*, *13*, 63–72. https://doi.org/10.14453/aabfj.v13i4.5

Fleming, S., Hermanson, D., Kranacher, M., & Riley, R. (2016). Financial reporting fraud: Public and private companies. *Journal of Forensic Accounting Research*, *1*, 27–41. https://doi.org/10.2308/jfar-51475

Frazer, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance*, *16*, 149–161. http://www.na-businesspress.com/jafopen.html

Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *UNSW Australia Business School, School of Accounting*, 1–37. http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2590952

Free, C., & Murphy, P. (2015). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research*, *32*(1), 18–54. https://doi.org/10.1111/1911-3846.12063

Gallagher, M., & Radcliffe, V. S. (2002). Internal controls in nonprofit organizations: The case of the American Cancer Society, Ohio division. *Nonprofit Management and Leadership*, *12*(3), 313–325. https://doi.org/10.1002/nml.12307

Galletta, P. (2015). A basic field guide to fraud. *The CPA Journal*, *85*, 54–59. https://www.cpajournal.com

García-Sánchez, P., Díaz-Díaz, N. L., & De Saá-Pérez, P. (2019). Social capital and knowledge sharing in academic research teams. *International Review of Administrative Sciences*, *85*(1), 191–207. https://doi.org/10.1177/0020852316689140

Garven, S. (2015). The basics about nonprofits: A beginner's guide for CPAs. *CPA Journal*, *85*(6), 18–19. https://www.questia.com/library/p61591/the-cpa-journal/i3821420/vol-85-no-6-june

Garven, S., Beck, A., & Parsons, L. (2018). Are audit-related factors associated with financial reporting quality in nonprofit organizations?. *Auditing: A Journal of Practice and Theory*, *37*, 49–68. https://doi.org/10.2308/ajpt-51819

Gibbs, G. R. (2007). Analyzing qualitative data. In U. Flick (Ed.), *The Sage qualitative research kit.* Sage.

Gray, D., & Villamarin, R. (2015). Stopping financial fraud in churches. *World Journal of Business and Management*, *1*(2). https://doi.org/10.5296/wjbm.v1i2.8162

Grbich, C. (2013). *Qualitative data analysis: An introduction* (2nd ed.). Sage.

Greenlee, J., Fischer, M., Gordon, T., & Keating, E. (2007). An investigation of fraud in nonprofit organizations: Occurrences and deterrents. *Nonprofit and Voluntary Sector Quarterly*, *36*(4), 676–694. https://doi.org/10.1177/0899764007300407

Gregory, E. M. (2017). *Exploring cash fraud awareness in nonprofit organizations* (Publication No. 10262437) [Doctoral dissertation, Capella University]. https://www.proquest.com/openview/6eac70eb1771dcdab5a00e47b52c4798/1?pq-origsite=gscholar&cbl=18750

Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: evidence from the UAE. *Managerial Auditing Journal*, *31*, 6–7. https://doi.org/10.1108/MAJ-02-2015-1163

Haislip, J. Z., Peters, G. F., & Richardson, V. J. (2016). The effect of auditor IT expertise on internal controls. *International Journal of Accounting Information Systems*, *20*, 1–15. https://doi.org/10.1016/j.accinf.2016.01.001

Hall, M., Barr, C., Easwaramoorthy, M., Sokolowski, S., & Salamon, L. (2005). *The Canadian nonprofit and voluntary sector in comparative perspective*. Imagine Canada, 1–39. Fremont-Smith,

Hare, R. D. (1999). *without conscience: the disturbing world of the psychopaths among us.* Guilford Press.

Harmon, M. M. (2011). Truth, telling the truth, and being truthful: Affect, nonverbal communication, and the constitution of ethical relationship. *Administrative Theory & Praxis*, *33*(4), 509–529. https://doi.org/10.2753/ATP1084-1806330401

Harris, E., Petrovits, C., & Yetman, M. H. (2017). Why bad things happen to good organizations: The link between governance and asset diversions in public charities. *Journal of Business Ethics*, *146*(1), 149–166. https://doi.org/10.1007/s10551-015-2921-9

Harrison, A., Summers, J., & Mennecke, B. (2018). The effects of the dark triad on unethical behavior. *Journal of Business Ethics*, *153*(1), 53–77. https://doi.org/10.1007/s10551-016-3368-3

Helge, T. L. (2017). Rejecting charity: Why the IRS denies tax exemption to 501(c)(3) applicants. *Pittsburgh Tax Review*, *14*(1). https://doi.org/10.5195/TAXREVIEW.2016.51

Hess, M., & Cottrell, J. (2016). Fraud risk management: A small business prospective. *Business Horizons*, *59*, 13–18. https://doi.org/10.1016/j.bushor.2015.09.005

Hill, M. (2016). The regulation of Christian churches: Ecclesiology, law and polity. *HTS Theological Studies*, *72*(1), 1–10. https://doi.org/10.4102/hts.v72i1.3382

Homer, E. (2020). Testing the fraud triangle: A systematic review. *Journal of Financial Crime*, *27*, 172–187. https://doi.org/10.1108/JFC-12-2018-0136

Hoos, F., & Bollmann, G. (2012). Is accountability a double-edged sword? Experimental evidence on the effectiveness of internal controls to prevent fraud. *Journal of Management Control*, *23*(2), 115–132. https://doi.org/10.1007/s00187-012-0161-z

Huber, D. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, *12*, 28–49. http://jtar.org

Hughes, R. (2018). What comptrollers want. *The Armed Forces Comptroller*, *63*(4), 41–44.

Internal Control. (2020, October 15). *Merriam-Webster.com dictionary*. https://www.merriam-webster.com/dictionary/internal%20control

IRS. (2020, October 12). Instructions for form 990 return of organization exempt from income tax 2019. www.irs.gov/instructions/i990.

Jankowski, P. (2019). Houston population expected to exceed 7.1 million by 2020. *Greater Houston Partnership*. https://www.houston.org/news/houston-population-expected-exceed-71-million-2020#:~:text=Metro%20Houston%20added%20nearly%2092%2C000,the%20end%20of%20the%20decade.

Jeavons, T. H. (2001). Ethics in nonprofit management. In J. S. Ott (Ed.), *Understanding nonprofit organizations: Governance, leadership and management* (pp. 108–119). Westview Press Jones.

Jeong, Y., & Siegel, J. I. (2018). Threat of falling high status and corporate bribery: Evidence from the revealed accounting records of two South Korean presidents. *Strategic Management Journal*, *39*(4), 1083–1111. https://doi.org/10.1002/smj.2747

Johansson, E., & Carey, P. (2016). Detecting fraud: The role of the anonymous reporting channel. *Journal of Business Ethics*, *139*(2), 391–409. https://doi.org/10.1007/s10551-015-2673-6

Johnson, T. M., Zurlo, G. A., & Hickman, A. W. (2015). Embezzlement in the global Christian community. *The Review of Faith and International Affairs*, *13*(2), 74–84. https://doi.org/10.1080/15570274.2015.1039302

Jones, D. N., & Paulhus, D. L. (2009). Machiavellianism. In M. R. Leary & R. H. Hoyle (Eds.), *Handbook of individual differences in social behavior* (pp. 93–108). The Guilford Press.

Kamaliah, K., Marjuni, N., Mohamed, N., Mohd-Sanusi, Z., & Anugerah, R. (2018). Effectiveness of monitoring mechanisms and mitigation of fraud incidents in the public sector. *Adminisrtatie Si Management Public*, *30*, 82–95. https://doi.org/10.24818/amp/2018.30-06

Kapardis, M., & Papastergiou, K. (2016). Fraud victimization in Greece: Room for improvement in prevention and detection. *Journal of Financial Crime*, *23*, 481–500. https://doi.org/10.1108/JFC-02-2015-0010

Kazantseva, A., & Plotnikov, V. (2018). Development of internal control system in the modern companies: Theoretical approaches and suggestions for improvement. *Administrative Consulting*, *10*, 99–108. https://doi.org/10.22394/1726-1139-2018-10-99-108

Kelly, M. (2017, September 14). Shameless self-promotion: Anti-fraud triangle paper. *Radical Compliance.* http://www.radicalcompliance.com/2017/09/14/promotion-anti-fraud-triangle-paper/

Kramer, B. (2015). Trust, but verify: fraud in small businesses. *Journal of Small Business and Enterprise Development*, *22*, 4–20. https://doi.org/10.1108/JSBED-08-2012-0097

Kummer, T., Singh, K., & Best, P. (2015). The effectiveness of fraud detection instruments in not-for-profit organizations. *Managerial Auditing Journal*, *30*, 435–455. https://doi.org/10.1108/MAJ-08-2014-1083

Latan, H., Chiappetta Jabbour, C. J., & Lopes de Sousa Jabbour, A. B. (2019). Whistleblowing triangle: Framework and empirical evidence. *Journal of Business Ethics*, *160*(1), 189–204. https://doi.org/10.1007/s10551-018-3862-x

Le, T., & Tran, M. (2018). The effect of internal control on asset misappropriation: The case of Vietnam. *Business and Economics Horizons*, *14*, 941–953. https://doi.org/10.15208/beh.2018.64

Leedy, P. D., & Ormrod, J. E. (2019). *Practical research*. Holt, Rinehart, and Winston.

Leland, P. J. (1996). Exploring challenges to nonprofit status: Issues of definition and access in community-based research. *The American Behavioral Scientist (Beverly Hills)*, *39*(5), 587–601. https://doi.org/10.1177/0002764296039005006

Lenz, P., & Graycar, A. (2016). Stealing from the boss: Who is looking?. *Journal of Financial Crime*, *23*, 613–623. https://doi.org/10.1108/JFC-09-2015-0053

LeVasseur, J. J. (2003). The problem of bracketing in phenomenology. *Qualitative Health Research*, *13*(3), 408–420. https://doi.org/10.1177/1049732302250337

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum*, *39*(3), 201–224. https://doi.org/10.1016/j.accfor.2015.05.002

Mangala, D., & Kumari, P. (2015). Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce and Accounting Research*, *4*, 52–62. http://www.publishingindia.com

Marks, J. T., & Ugo, P. A. (2020, October 10). *A violation of trust: Fraud risk in nonprofit organizations.* Nonprofit Risk Management Center.

Mayo Clinic. (2020, October 26). *Diseases and conditions*. https://www.mayoclinic.org/diseases-conditions

McMahon, R., Pence, D., Bressler, L., & Bressler, M. (2016). New tactics in fighting financial crimes: Moving beyond the fraud triangle. *Journal of Legal, Ethical and Regulatory Issues*, *19*, 16–25. https://www.abacademies.org/articles/jlerivol19number1.pdf

Meckstroth, A., & Arnsberger, P. (1998). A 20-year review of the nonprofit sector, 1975–1995. *SOI Bulletin*, *18*, 149–169. https://www.irs.gov/pub/irs-soi/20yreo.pdf

Meinert, M. C. (2016). In the fight against fraud, strong leadership is key. American Bankers Association. *ABA Banking Journal*, *108*(2), 55. http://bankingjournal.aba.com

Moore, J. (2018). The relationship between organization size and occupational fraud. *International Research Journal of Applied Finance*, *9*, 248–276. http://www.irjaf.com

Moustakas, C. (1994). *Phenomenological research methods.* Sage.

Mui, G., & Mailley, J. (2015). A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle. *Accounting Research Journal*, *28*(1), 45–58. https://doi.org/10.1108/ARJ-10-2014-0092

Murphy, M. (2015). Preventing and detecting fraud at not-for-profits. *Journal of Accountancy*, *220*, 77–83. https://www.journalofaccountancy.com/

Murphy, P., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting*, *28*, 41–56. https://doi.org/10.2308/bria-51083

Nawawi, A., & Salin, A. (2018). Employee fraud and misconduct: Empirical evidence from a telecommunication company. *Information and Computer Security*, *26*, 129–144. https://doi.org/10.1108/ICS-07-2017-0016

NCCS. (2020, October 20). The nonprofit sector in brief 2019. *National Center for Charitable Statistics*. https://nccs.urban.org/publication/nonprofit-sector-brief-2019#notes

New International Version Bible. (2011). The NIV Bible. https://www.thenivbible.com (Original work published 1978)

Nørreklit, H., Nørreklit, L., & Mitchell, F. (2016). Understanding practice generalization – opening the research/practice gap. *Qualitative Research in Accounting and Management*, *13*(3), 278–302. https://doi.org/10.1108/QRAM-09-2015-0088

Office for Human Research Protections. (2021, January 22). *The Belmont Report*. U.S. Department of Human and Health Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Ohalehi, P. (2019). Fraud in small charities: Evidence from England and Wales. *Journal of Financial Crime*, *26*, 211–222. https://doi.org/10.1108/JFC-12-2017-0122

Omar, M., Nawawi, A., & Salin, A. (2016). The causes, impact and prevention of employee fraud: A case study of an automotive company. *Journal of Financial Crime*, *23*, 1012–1027. https://doi.org/10.1108/JFC-04-2015-0020

Othman, R., & Ali, N. (2014). NPO, internal controls, and supervision mechanisms in a developing country. *Voluntas*, *25*(1), 201–224. https://doi.org/10.1007/s11266-012-9335-4

Park, Y., Matkin, D., & Marlowe, J. (2017). Internal control deficiencies and municipal borrowing costs. *Public Budgeting and Finance*, *37*, 88–111. https://doi.org/10.1111/pbaf.12120

Pedneault, S. (2010). *Preventing and detecting employee theft and embezzlement: A practical guide.* John Wiley and Sons.

Peltier-Rivest, D. (2018). The battle against fraud: Do reporting mechanisms work?. *Journal of Financial Crime*, *25*, 784–794. https://doi.org/10.1108/JFC-05-2017-0048

PwC. (2020 October 15). Global economic crime and fraud survey 2020. *PricewaterhouseCoopers.* https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

Purnamasari, P., & Amaliah, I. (2015). Fraud prevention: Relevance to religiosity and spirituality in the workplace. *Procedia-Social and Behavioral Sciences*, *211*, 827–835. https://doi.org/10.1016/j.sbspro.2015.11.109

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. *Australasian Accounting, Business and Finance Journal*, *11*(1), 28–54. https://doi.org/10.14453/aabfj.v11i1.4

Reinstein, A., & Taylor, E. Z. (2017). Fences as controls to reduce accountants' rationalization. *Journal of Business Ethics*, *141*(3), 477–488. https://doi.org/10.1007/s10551-015-2701-6

Ries, R. (2016). How to evaluate risk in the modern not-for-profit industry. *The CPA Journal*, *86*, 6–7. https://www.cpajournal.com

Riessman, C. K. (2008). *Narrative methods for the human sciences.* Sage.

Rijsenbilt, A., & Commandeur, H. (2017). Narcissus enters the courtroom: CEO narcissism and fraud. *Springer Stable*, *117*(2), 413–429. http://www.jstor.org/stable/42001858

Rockson, A. (2019). *Strategies for preventing financial fraud in church organizations in Ghana* (Publication No. 13901488) [Doctoral *Dissertation*, Walden University]. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=8386&context=dissertations

Ruankaew, T. (2016). Beyond the fraud diamond. *International Journal of Business Management and Economic Research*, *7*, 474–476. https://www.ijbmer.com

Rubasundram, G. A. (2015). Perceived “tone from the top” during a fraud risk assessment. *Procedia Economics and Finance*, *28*, 102–106. https://doi.org/10.1016/S2212-5671(15)01087-4

Schnatterly, K., Gangloff, K., & Tuschke, A. (2018). CEO wrongdoing: A review of pressure, opportunity, and rationalization. *Journal of Management*, *44*, 2405–2432. https://doi.org/10.1177/0149206318771177

Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, *29*(2), 107–121. https://doi.org/10.1057/sj.2013.1

Schuchter, A., & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, *39*(3), 176–187. https://doi.org/10.1016/j.accfor.2014.12.001

Simha, A., & Satyanarayan, S. (2016). Straight from the horse’s mouth: Auditor’s on fraud detection and prevention, roles of technology, and white-collars getting splattered with red!. *Journal of Accounting and Finance*, *16*, 26–44. http://www.na-businesspress.com

Snyder, H., Andersen, M., & Zuber, J. (2017). Nonprofit fraud: How good are your internal controls? *Strategic Finance*, *98*(9), 54–62. https://sfmagazine.com

Soobaroyen, T., & Sannassee, R. (2007). An exploratory study of financial priorities, financial planning and control practices in voluntary organisations: Perceptions of treasurers in a developing country. *Journal of Accounting & Organizational Change*, *3*(3), 270–301. https://doi.org/10.1108/18325910710820300

Sorsa, M., Kiikkala, I., & Åstedt-Kurki, P. (2015). Bracketing as a skill in conducting unstructured qualitative interviews. *Nurse Researcher*, *22*(4), 8–12. https://doi.org/10.7748/nr.22.4.8.e1317

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*, *6*(2), 159–165. https://doi.org/10.6007/IJARBSS/v6-i2/2020

Stake, R. E. (1995). *The art of case study research.* Sage.

Stake, R. E. (2010). *Qualitative research: Studying how things work*. Guilford Press.

Sun, P. Y. T., & Anderson, M. H. (2012). Civic capacity: Building on transformational leadership to explain successful integrative public leadership. *The Leadership Quarterly*, *23*(3), 309–323.

Todd, K. (2016). *Why corruption always requires a conflict of interest.* http://www.forensicstrategic.com/blog/why-corruption-always-requires-a-conflict-of-interest

Tremblay-Boire, J., & Prakash, A. (2015). Accountability.org: Online disclosures by U. S. nonprofits. *Voluntas: International Society for Third-Sector Research*, *26*, 693–719. https://doi.org/10.1007/s11266-014-9452-3

Wells, J. T. (2014). *Principles of fraud examination* (4th ed.). John Wiley.

Wilkinson, B. R. (2005). A framework for a Christian perspective on accounting research. *Journal of Biblical Integration in Business*, *11*(1), 57–79. https://cbfa-jbib.org/index.php/jbib/article/view/255

Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, *74*(12), 38–42. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). The Guilford Press.

Yin, R. K. (2018). *Case study research and applications: Design and methods*. Sage.

Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2005). The antecedents and consequences of top management fraud. *Journal of Management*, *31*(6), 803–828. https://doi.org/10.1177/0149206305279598

Zakaria, K., Nawawi, A., & Salin, A. (2016). Internal controls and fraud – empirical evidence from oil and gas company. *Journal of Financial Crime*, *23*, 1154–1168. https://doi.org/10.1108/JFC-04-2016-0021

Appendix A: Pre-Interview Survey

1. What is your name?
2. What organization are you currently employed or volunteer with?
3. How long have you worked or volunteered at your current organization?
4. How many years of work experience do you have with nonprofits?
5. How many years of work total experience in your field do you have?
6. What is your gender?
7. What is your highest level of education?
8. Do you have any advanced certificates (such as CPA)?
9. What practices or policies does your organization use to prevent or detect fraud?
    a. Does your organization have an annual external audit? Attach copy of audit report.
    b. Does your organization have a fraud control policy or internal controls policies and procedures? Attach copy of policy.
    c. Does your organization have a code of conduct? Explain or attach copy of policy.
    d. Does your organization have a whistleblower policy? Explain or attach copy of policy.
    e. Does your organization have an internal audit department? Explain.
    f. Does your organization conduct background checks on employees? Explain.
    g. Has your organization done an assessment of the risk of fraud? Explain.
10. Please upload a copy of your organization's financial statements, annual report, or Form 990.

Appendix B: Interview Guide

1. What is your name and position in this organization?
2. What are your primary duties and responsibilities for this organization?
3. What strategies does your organization use to lower the risk of fraud?
4. How does your organization assess the effectiveness of the strategies to lower the risk of fraud?
5. What practices or policies does your organization use to prevent or detect fraud?
6. What type of internal controls processes does your organization have to detect or prevent fraud?
    a. Is there a process for collecting revenue, donations, or gifts? Explain.
    b. Is there a process for making payments with cash, check, or electronically? Explain.
    c. Are there controls related to accounting data and reporting? Explain.
7. Has your organization experienced any inadvertent use of funds, funds used incorrectly, waste of funds, or fraud within the past 10 years?
8. What strategy or internal control do you believe has been the most successful in detecting or preventing fraud and why?
9. What strategies or internal controls do you believe your organization should implement to further deter and detect fraud?
10. What additional information can you add that was not already discussed?

Appendix C: Copyright Permission

ACFE Report to the Nations Permission

Re: ACFE Report to the Nations - Image Permission
Isaiah Sosa
Tue 1/25/2022 4:23 PM
To: Miller, Shawn Thomas

Hi Mr. Miller,

Thank you for contacting the Association of Certified Fraud Examiners (ACFE). We appreciate your inquiry to the ACFE, I am more than happy to assist you. Yes, you can include graphics from the 2020 ACFE Report to Nations as long as the ACFE is credited.
You can click here to access our ACFE Brand Standards templates and logos.
If you have any further questions or concerns, please feel free to contact me directly.

Best Regards,

Isaiah Sosa
Member Services Representative
Association of Certified Fraud Examiners

From: "Miller, Shawn Thomas"
Date: Monday, January 24, 2022 at 11:14 AM
To: MEMBERSERVICES
Subject: ACFE Report to the Nations - Image Permission

ACFE,

My name is Shawn Miller, and I am a doctoral student at Liberty University. I would like to include a graphic from the 2020 ACFE Report to the Nations. This graphic is the Fraud Tree on page 11. Would you please give me permission to publish this in my dissertation.
Thank you,

Shawn Miller

COSO Framework Permission

Copyright Permissions
Mon 1/31/2022 3:31 PM
To: Miller, Shawn Thomas

Hi Shawn,
Thank you for reaching out. Consider this email as proof of granting permission.
Best regards,

Kyle George
Sr. Manager – Licensing & Rights

From: Miller, Shawn Thomas
Sent: Wednesday, January 26, 2022 6:58 PM
To: COPYRIGHT
Subject: Copyright Permission

AICPA,

My name is Shawn Miller, and I am a doctoral student at Liberty University. I would like toinclude a graphic of the COSO framework cube in my dissertation. This image is found on thispage:

https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

Would you please give me permission to publish this image in my dissertation.

Thank you,

Shawn Miller