AN EXPLORATION OF INTERNAL CONTROLS AND THEIR IMPACT ON EMPLOYEE FRAUD IN SMALL BUSINESSES

by

Kent Lachney

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University

May, 2018

Abstract

The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and to explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. The researcher selected five small businesses that were members of the Central Louisiana Regional Chamber of Commerce and had fewer than 100 employees. The researcher interviewed the owners and/or managers of the businesses, reviewed and analyzed company documentation, interpreted data, made observations, and offered recommendations. The researcher asked each participant to respond to questions related to the five elements of the model developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO): control environment, risk assessment, control activities, information and communication, and monitoring. The researcher discovered that there were more internal controls utilized by the businesses that participated in this study than were depicted in a review of current literature. Also, the researcher identified several themes of best practices of internal controls: anti-fraud training; written code of conduct; risk assessment; hiring and onboarding process; approval processes and authorization levels; separation of duties; information and communication; and monitoring. Further, the researcher made six recommendations for action: establishing internal controls; addressing personnel issues; conducting anti-fraud training; revising personnel manuals; assessing risk; and monitoring COSO standards. This study should assist small business owners and/or managers achieve their organization's objectives and make a significant contribution to the local economy.

Keywords: Association of Certified Fraud Examiners (ACFE), employee fraud, internal controls, Committee of Sponsoring Organizations of the Treadway Commission (COSO)

AN EXPLORATION OF INTERNAL CONTROLS AND THEIR IMPACT ON EMPLOYEE FRAUD IN SMALL BUSINESSES

by

Kent Lachney

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University

May, 2018

_____

Dr. Scott Ehrhorn, Dissertation Chair

_____

Dr. Gene Sullivan, Dissertation Committee Member

_____

Dr. Gene Sullivan, DBA Director

_____

Dr. David Calland, Interim Dean, School of Business

Dedication

I dedicate this doctoral research paper to my wife, Ronda, who encouraged me continuously throughout the doctoral process. Also, I dedicate this research to my two granddaughters, Hannah and Lydia, who serve as a constant joy to me. Their smiles and hugs are an inspiration to me.

Acknowledgments

I would like to thank my family, Ronda, Angela, Hannah, and Lydia for the many sacrifices they made while I pursued my education over the years. I would also like to thank my colleagues and administration at Louisiana State University at Alexandria for their encouragement, flexibility, and resources to allow me to complete this dissertation. Finally, I would like to thank my dissertation committee chair, Dr. Scott Ehrhorn, and committee member, Dr. Gene Sullivan, for their guidance throughout this journey

.

Table of Contents

Section 1: Foundation of the Study

Employee fraud frequently leads to disastrous results, particularly for small businesses which may not have the financial reserves to out-weigh its detrimental effects. These organizations usually do not have the resources available to implement extensive internal controls. Not only does fraud lead to a reduction in an organization's assets and income, but it can even result in its failure. Small businesses are often more directly impacted with the negative psychological and emotional aspects of a loss than their larger organizational counterparts because small business owners have greater feelings of personal betrayal. Assessing the current level of internal controls is the first step in assisting small business owners in developing skills and knowledge to reduce employee fraud.

Background of the Problem

Many small business owners fear bad publicity and cannot afford the time and expense of prosecution, so many instances of fraud are quietly dismissed. In addition, Kramer (2015) acknowledged that some fraud, particularly involving small businesses, is not reported to the Association of Certified Fraud Examiners (ACFE). The ACFE *Report to the Nations on Occupational Fraud and Abuse* (2016) described selected fraud statistics, which included the number of fraud occurrences, dollar amounts involved, and the type of frauds perpetrated. Employee fraud is difficult to detect because of the nature of concealment. Noviyanti and Winata (2015) found that most forensic accountants adhere to the 5/10/85 rule, which holds that 5% of employees will steal regardless of the circumstances, 10% will never steal, and 85% may commit fraud, depending on certain conditions. In fact, most small business owners think they are not at risk for fraud because of the "tone at the top" or climate of their organization; in essence, they disregarded the need for effective internal controls (Gagliardi, 2014, p. 11;

Noviyanti & Winata, 2015, p. 55). Further, Law and Kusant (2014) noted the lack of internal controls typically provide situations which lend themselves to fraudulent acts. Accordingly, the 5/10/85 rule may cause some small business owners to reconsider the possibility of employee fraud.

It is important for small business owners to better understand why and how employee fraud occurs. In his seminal work, Cressey (1950) identified three elements that must exist for employee fraud to occur. The three parts of the fraud triangle include incentive or motive, opportunity, and rationalization. If one element is absent, then the risk of fraud decreases significantly. Wolfe and Hermanson (2004) expanded on this work by proposing a fraud diamond in which personal and organizational factors formed a fourth dimension they called capability. Subsequently, Free (2015) and Yusof, Khair, and Simon (2015) described the fraud pentagon that further develops the original fraud triangle. The authors explained the fraud pentagon adds the elements of arrogance and competence. They described arrogance as an attitude of entitlement and superiority whereas competence refers to the perpetrator's ability to take advantage of his or her position in the organization and thereby circumvent internal controls. Accordingly, Lenz and Graycar (2016) acknowledged it is beneficial for small business owners to recognize the personal factors, such as an employee's position in the company, intelligence, and ego, that contribute to fraud. Lenz and Graycar (2016) also pointed out that owners and managers should be aware of organizational factors, such as poor management and lack of internal controls, which increase the risk for employee fraud to occur. By understanding the use of internal controls, employee fraud risk can be decreased.

Red flags or fraud risk indicators are also a concern to small business owners.

Gullkvist and Jokipii (2013) confirmed that red flags, such as personal characteristics, opportunities, and pressures, do not guarantee that fraud has occurred. However, they are an indication that internal controls should be investigated to determine if there are any weaknesses for which vulnerabilities are being exploited. There are numerous factors that small business owners can look for in an effort to become better aware of potential fraud.

Many types of fraud are perpetrated in small businesses. Kramer (2015) found that asset misappropriation is the most common type of employee fraud while other typical methods include skimming cash, overstating expense reimbursements, and tampering with checks. He found that check tampering occurs three times more frequently in smaller organizations than in larger ones. Consequently, Brody, Melendy, and Perri (2012) identified the need to evaluate the level of internal controls in small businesses and their effect on employee fraud risk. In addition, Law and Kusant (2014) found that small businesses with less than 100 employees suffered an average loss of $200,000 per incident. They recommended that research be conducted to develop internal control guidelines for small businesses so that the risk of employee fraud would be minimized. By comparing their internal controls with the most common types of fraud perpetrated in small businesses, owners will be able to better evaluate their level of fraud risk. It is important for small business owners to develop a strong grasp of effective internal control practices to minimize employee fraud risk. There is a lack of research concerning fraud in small businesses; consequently, further research is needed.

Problem Statement

The general problem addressed was the internal controls employed by small businesses are ineffective and lead to higher levels of employee fraud risk. Brody et al. (2012) documented the importance of evaluating the level of internal controls in small businesses and determine their

effect on employee fraud risk. Likewise, Law and Kusant (2014) pointed out the lack of internal controls frequently provide situations which lend themselves to fraudulent acts. Therefore, the authors encouraged researchers to conduct studies to develop internal control guidelines for small businesses so that the risk of employee fraud would be minimized. However, there is a lack of such research. Researchers have conducted few studies on the exploration of internal controls in small businesses and their impact on employee fraud risk. In fact, the Institute for Fraud Prevention listed only one study in the United States concerning ineffective internal controls in small businesses since 2006 (Institute for Fraud Prevention, 2016). Specifically, the focus of this study was to explore the internal controls of small businesses which had fewer than 100 employees and that were members of the Central Louisiana Regional Chamber of Commerce located in Alexandria, Louisiana, in an effort to mitigate employee fraud risk. According to Wilkins and Haun (2014), many small business organizations view internal controls as expensive and unnecessary. Wilkins and Haun (2014) explained that too often, business owners think of internal controls as a means of security rather than as a system of achieving organizational goals and minimizing errors. Accordingly, the authors cited examples of how the internal controls in many small businesses are ineffective. In addition, Rittenberg (2006) described how many smaller organizations face issues, such as effectively using information technology and efficiently attaining the proper level of financial competence. Awareness is the first step in fraud prevention. Hall (2016) described the importance of managers and owners knowing what to look for in the anti-fraud moment which is when they review and approve transaction documents. In a recent UK study, Elvin (2015) suggested that increased internal controls would prevent at least 77% of workplace fraud. Proper internal controls play a vital role in the success of small businesses.

Purpose Statement

The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of select small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. Effective internal controls are the first step of defense against employee fraud. Dimitrijevic, Milovanovic, and Stancic (2015) posited that the risk of employee fraud could be minimized through the implementation of effective internal controls. Further, Tschakert, Needles, and Holtzblatt (2016) emphasized the importance of owners and managers being able to recognize red flags, which frequently result from ineffective internal controls. Consequently, weak internal controls and managers' lack of knowledge of red flags lead to an increased risk from employee fraud. Simha and Satyanarayan (2016) concluded that small business organizations are less likely to invest in the resources of time and money to set-up internal controls than their larger counterparts. They emphasized that investing in fraud prevention education and techniques is essential to decreasing employee fraud risk.

Nature of the Study

During this study, the researcher explored the internal controls of several small businesses. The researcher employed the qualitative method, case study design to interpret data, make observations, and offer recommendations. The qualitative research method was most suitable for this study because this methodology utilizes observation and interpretation whereas the quantitative and mixed method research involves measurable variables and numerical data. Houghton, Murphy, Shaw, and Casey (2014) and Guercini (2014) posited that the qualitative research method is appropriate to study situations, events, programs, and activities in their natural settings. Although qualitative research is flexible in its implementation, it is thorough in

acquiring a comprehensive understanding of the subject (Houghton et al., 2014; Guercini, 2014). Sorour and Howell (2013) asserted that qualitative research goes beyond snapshots of *what* or *how many* to actually determining *how* and *why* things happen. The qualitative method allows for researchers to be creative and flexible as it focuses on several aspects of a study simultaneously.

To properly conduct qualitative research, the investigator must adopt a different mindset. Kaczynski, Salmona, and Smith (2014) shared that research must extend beyond simple data collection to include the exploration of a greater understanding of relationships. Researchers should include the adoption of a concept that Geertz (1973) referred to as "researcher as instrument." The investigator and the research are interwoven so the examiner should contemplate what they individually bring to the research and their role throughout the process (Geertz, 1973). Further, Yin (2014) argued the ability for researchers to incorporate their experience into a study unites business studies to social sciences such as anthropology, history, psychology, political science, and sociology as well as the fields of education and nursing. Although qualitative research has been criticized by some researchers who believe this type of research lacks scientific value, it has increased in its use because the qualitative method adds a much needed personal interpretation to the study. It is because of the researchers' comprehensive mindset that investigators gain a more thorough understanding of the phenomena being studied.

In addition to the qualitative approach, researchers may choose to use the quantitative or mixed method research method in their study. Quantitative business research focuses on objectives that involve numerical assessment and analysis in which the goal is to quantify data and measure the instances of certain viewpoints. Zikmund, Babin, Carr, and Griffin (2012)

pointed out that one challenge of using quantitative research is that it involves considerable time in developing assessment instruments that contain numerical values which are used in statistical computations and testing hypotheses. The quantitative method is more objective in nature than qualitative research since it relies on statistics whereas qualitative does not. Quantitative research is structured, conclusive, and used to recommend a course of action (Park & Park, 2016). Further, Buckley (2015) indicated the quantitative method answers the information-gathering, interrogative question of *what* rather than *why* or *how*, as used in the qualitative research approach. Since the purpose of this study was to determine *how* small businesses apply internal controls to mitigate employee fraud risk, the quantitative method was not appropriate for use in this study.

The mixed methods research (MMR) approach combines elements from both qualitative and quantitative research. Creswell, Shope, Clark, and Green (2006) contended the main principle of MMR is that both approaches used together provide a better understanding of the research problem than either single approach. Further, Venkatesh, Brown, and Bala (2013) reported that typically, quantitative methods are used for confirmatory studies to test hypotheses whereas qualitative methods are used to explore a topic. Mixed method research allows the strengths of each approach to compensate for the weaknesses of both qualitative and quantitative research. Creswell (2014) clarified that the mixed method approach is appropriate to use when the researcher has the supposition that collecting diverse types of data provides a more complete understanding of a research problem than either quantitative or qualitative data alone. Creswell (2014) explained the study has two phases. The first phase is a quantitative, broad survey to generalize results to a population, and the second phase focuses on qualitative, open-ended interviews to collect detailed views from participants. In this study, the researcher did not use

numerical data or tested hypotheses. Since the purpose of the study was to gain greater understanding of the current internal control practices of small business organizations and to explore the effectiveness of their systems, the mixed method approach was not appropriate.

The purpose of a research design is to ensure the data gathered enables the researcher to effectively address the study's problem and answer the research questions. Singh (2014) identified five designs that researchers may use to frame their qualitative inquiry: case study, ethnography, phenomenology, grounded theory, and narrative.

The case study design in qualitative research is used when a researcher wants to gain an in-depth understanding of an individual, family, or organization. Singh (2014) pointed out that this is the preferred method when the investigator is seeking to determine the answers to *how* and *why* questions rather than manipulate variables in a study. Although Stake (2005) viewed case study as a choice of *what* is to be studied rather than *how* it is studied, Creswell (2013) believed it is a methodology. Moreover, Stake (2005) emphasized that case studies gain reliability by meticulously triangulating the reports and interpretations continuously throughout study. Stake (2005) clarified that the case study approach concentrates on empirical knowledge of the case. Creswell (2013) and Stake (2005) explained the case study design utilizes multiple sources of information, such as documentation, interviews, and direct- and participant-observation as means to gather data. In addition, Cleary, Horsfall, and Hayter (2014) emphasized the importance of engaging and communicating with the participant to receive the most comprehensive interview responses. Further, Starman (2013) and Yin (2014) acknowledged that case studies have been used in social sciences and are valued in practice-oriented fields, such as education, public administration, and management. Guercini (2014) also acknowledged the case study method has

increased in popularity, especially in industrial marketing, management, and entrepreneurship research.

Other types of qualitative design include ethnography, phenomenology, grounded theory, and narrative. Ethnographic research is probably the most familiar design of qualitative research. According to Cordoba-Pachon and Loureiro-Koechlin (2015) and Grossoehme (2014), in this type of study, which began in the field of anthropology, a researcher engages himself in the participant's environment to understand the culture, goals, and challenges in that situation. Cordoba-Pachon and Loureiro-Koechlin (2015) and Grossoehme (2014) explained that this type of research is not based on simple interviews, but observations that may require years for the researcher to become fully immerged in the setting. Creswell (2013) pointed out that in an ethnography, the researcher explains and interprets the learned patterns of behaviors, beliefs, language, and values of an entire culture-sharing group, people who interact over time. A phenomenological study is the appropriate qualitative method to use when the researcher wants to describe an activity, event, or a phenomenon based on the participant's experience. Snelgrove (2014) and Mosalanejad, Paransavar, Gholami, and Abdellahifard (2014) explained that through interviews, watching videos, reading documentation, visiting locations, or participating in events, the researcher can gain an understanding of the participant's perception of an event. Snelgrove (2014) and Mosalanejad et al. (2014) highlighted its subjective nature of research. However, this is the best method to use when one wants to study what an experience or event means to a particular person or group of people. While a phenomenological study is used to describe an event, the grounded theory approach provides a theory or explanation of why an event occurs. Glaser (2014) described the theory he and Anselm Strauss developed in 1967 in the field of sociology. Glaser (2014) emphasized that grounded theory enables the researcher to see a

situation as it actually exists without prejudice. Likewise, Webster (2016) clarified that this technique is inductive in nature in that it permits the researcher to examine the means that their subjects utilize to solve their concerns. A benefit of using grounded theory is it adopts a neutral view of human actions by avoiding researcher assumptions. Creswell (2013) explained that grounded theory is the best approach to use when a theory is not available to understand or explain the steps in a process. In the narrative method of qualitative research, researchers limit the study to one or two people in order to develop a persona. Jeppesen (2016) clarified that with the narrative design, researchers use ordinary literary methods to create a story that interweaves a sequence of events. Narrative research is typically used in the sciences, particularly in describing health issues.

After reviewing the five research designs, the researcher determined that the most valid and reliable method of qualitative research was the case study approach. Case studies are best to conduct an in-depth study of contemporary phenomena. This type of research answers the questions of *how* and *why*, which is best for this study of fraud risk in small business organizations. Also, since the researcher does not control the variables, case study was the best approach. In addition, the investigator conducted multiple case studies and ultimately draw cross-set conclusions.

Research Question

Ineffective internal controls employed by small businesses lead to increased levels of employee fraud risk. Brody et al. (2012) identified the need to evaluate the level of internal controls in small businesses and their effect on employee fraud risk. In addition, Law and Kusant (2014) recommended that research be conducted to develop internal control guidelines for small businesses so that the risk of employee fraud would be minimized. The purpose of this

multi-case study was to gain a greater understanding of the current practices of the internal control systems of selected small businesses and explore the effectiveness of their systems. Accordingly, the central research question was: "How do small businesses in Central Louisiana apply internal controls to mitigate employee fraud risk?" Further, the sub-question was "How do these small businesses meet the standards established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which included five elements: control environment, risk assessment, control activities, information and communication, and monitoring?"

Conceptual Framework

Weak internal controls lead to increased fraud risk. Therefore, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the Internal Control-Integrated Framework (ICIF) in 1992 and published revisions in 2013. The five components of the model are control environment, risk assessment, control activities, information and communication, and monitoring. The control environment, which focuses on risk management culture within organizations, forms the foundation for the other four elements. All organizations, regardless of size, are faced with both internal and external risks that may affect the entities' objectives. Risk assessments are necessary to identify relevant risks and determine how the organization can best manage the risks. Control activities refer to the policies and procedures of an organization, including the hiring, onboarding, and training process; approval processes; security of assets; authorization levels; and the segregation of duties. The information and communication component of the COSO model emphasizes the importance of organizations generating and using pertinent information to support the effectiveness of internal controls. Monitoring can be defined as performing assessments to determine if the five components of

internal controls are present and operational (Henry, 2016; Pett, Blomster, & Wallace, 2015; Rae, Sands, & Subramaniam, 2017; Wilkins & Haun, 2014).

In addition, the COSO developed the Enterprise Risk Management (ERM) Integrated Framework. McNally (2015) described the 2004 ERM framework as a complementary model to the COSO's internal control framework, which provides guidance to business organizations in an effort to help them develop and apply their enterprise risk management activities. McNally (2015) explained that in addition to some of the components of the ICIF, the ERM framework added objective setting and expanded the risk assessment component into three areas: event identification, risk assessment, and risk response. Verovska (2014) argued that the choice of internal controls depends upon the complexity of the organization's structure as well as its legal form, type of industry, and management's attitude concerning internal control. Further, Rittenberg (2006) advised that three factors should be considered before implementing a particular internal control. Rittenberg recommended that organizations should consider if (a) it reduces risk to a satisfactory level, (b) is cost effective, and (c) it is one of the COSO framework's five components of effective internal control.

The International Organization for Standardization (ISO) published Standard 31000 in 2009, which provides principles and guidelines of risk management in order to help businesses achieve their objectives, identify threats, and allocate resources for risk management. Effective risk management creates value and is an essential part of organizational procedures and decision making, and focuses on uncertainty. Effective risk management must be structured, systematic, timely, and dynamic. It also must be tailored to an organization's unique circumstances, responsive to change and be transparent and inclusive. Finally, effective risk management must facilitate continuous improvement. The COSO and the ISO both offer frameworks that improve

the effectiveness of organizational risk management and internal control activities (McNally, 2015).

There are a number of fraud risk assessment models that aid criminologists, forensic accountants, and auditors in helping their clients prevent fraud in their organizations. The foundation for these models was laid through the seminal work of Sutherland (1940), in which he compared business crime committed by respected businessmen, the white-collar or upper class, with crime committed by persons of low socioeconomic status. Sutherland's seminal research led to many models that focused on white-collar crime, including the further development of his theories by one of his doctoral students. Cressey (1950) formulated the fraud triangle, in which he hypothesized three components must be present for people to commit fraud, pressure (incentive), opportunity, and rationalization. Also, Trompeter, Carpenter, Desai, Jones, and Riley (2013) emphasized the fraud triangle represented the actions of the fraudster prior to committing the fraud, in which the perpetrator assessed the number of anti-fraud measures in place and then determined whether he/she could successfully execute and conceal the fraudulent actions. Cressey's research has served as a basis to further develop the fraud model, which aides in fraud prevention and detection. For example, Wolfe and Hermanson (2004) postulated the fraud diamond added a fourth dimension, capability. They argued that perpetrators must have the skills and ability necessary to commit the fraud.

The fraud pentagon is another transformation of the fraud triangle. In this model, the five elements are pressure, opportunity, rationalization, competence or the power for an employee to perform fraudulent acts, and arrogance or lack of conscience (Free, 2015; Playing offence in a high-risk environment, n.d; Yusof et al., 2015).

The fraud scale was developed by Mackevičius and Girūnas (2013) and included the elements of motives, conditions, possibilities, and realization. Mackevičius and Girūnas explained that all of these components are related to internal controls. Motive refers to a fraudster's incentive to commit fraud. Conditions refer to the circumstances necessary for fraud to occur, which include the activities, accounting, and internal controls of the organization. Mackevičius and Girūnas explained that possibilities are affected by the perpetrator's position in the company, access to assets and accounting records, and knowledge of internal controls. The final element, realization, includes the fraudster's personal characteristics, such as integrity allows the perpetrator to objectively evaluate his willingness to commit the fraud rather than only justifying the crime.

The fraud cycle begins with the fraud triangle, which is considered pre-fraud actions. Steven Albrecht developed the triangle of fraud action, the post-fraud functions of the criminal act (Albrecht, Albrecht, Albrecht, & Zimbelman, 2012). The triangle of fraud action is used to explain the fraudulent act, concealment of the crime, and conversion to a usable form for the perpetrator (McMahon, Pence, L. Bressler, and M. Bressler, 2016; Trompeter et al., 2013).

The fraud triangle and the triangle of fraud action are combined to form the meta-model of fraud, a comprehensive model that relates a potential fraudster's internal perceptions to the actions necessary to complete the fraud successfully. Dorminey, Fleming, Kranacher, and Riley (2012) indicated the meta-model assists fraud prevention specialists understand how to prevent, deter, detect, and investigate fraud in a more comprehensive manner. Trompeter et al. (2014) explained that between the fraud triangle and the elements of fraud lies the anti-fraud measures, such as internal controls.

Other researchers have developed theories that more fully explain the elements of pressure and opportunity. For example, Agnew (2015) explained the element of pressure in terms of the general strain theory (GST), which holds that people engage in criminal activities because they suffer from certain stressors or strains. Agnew reasoned that these strains usually involve the inability to achieve certain goals, such as freedom from monetary issues, which result in negative emotions, such as frustration and anger. Consequently, these emotions create pressure to correct the issue, and some people turn to crime as the answer. To explain the opportunity aspect of the fraud triangle, Cohen and Felson (1979) proposed the routine activities theory (RAT), which focuses on instances in which perpetrators carry out intentional, destructive criminal acts. Moreover, Argun and Dağlar (2016) pointed out that factors necessary to commit a crime include a motivated perpetrator who has an unguarded target. The authors explained that the routine activity theory is based on the belief that one of the most neglected aspects in sociological crime research is the issue of ordinary citizens guarding other people and their property. In addition, Trompeter et al. (2013) emphasized the importance of reducing or eliminating the opportunity for fraud by increasing internal controls, emphasizing the organization's ethical culture, and looking for red flags. Trompeter et al. (2013) emphasized that these factors significantly reduce the opportunity for employee fraud. By understanding the pressures that potential fraudsters have and opportunities that small businesses may present to commit dishonest acts, business owners can initiate internal controls that can reduce the potential for fraud.

There is a lack of research concerning the prevention of fraud in small businesses. Although there has been extensive research conducted to determine the personality traits and characteristics of fraudsters, there is minimal research regarding the internal controls employed

by small businesses as they relate to employee fraud risk. This research study helped in filling that gap.

Definition of Terms

Fraud triangle: Cressey (1950) proposed the fraud triangle in which three conditions must be present for fraud to occur: pressure (incentive), opportunity, and rationalization.

Internal control: Spiceland, Sepe, Nelson, and Thomas (2014) identified internal control as "a company's plan to (a) encourage adherence to company policies and procedures, (b) promote operational efficiency, (c) minimize errors and theft, and (d) enhance the reliability and accuracy of accounting data."

Occupational fraud: Singh, Best, and Mula (2013) described white-collar or occupational fraud as "financially oriented offenses committed by individuals within the context of a legitimate occupation and especially made possible by that occupation" (p. 615). In addition, Lenz and Graycar (2016) quantified that occupational fraud is usually committed by "higher class individuals," such as people who are in high management positions and may not be directly employed by the organization (p. 615).

Tone at the top: Patelli and Pedrini (2015) defined tone at the top as an atmosphere created by owners, board of directors, or chief executive officers.

Assumptions, Limitations, and Delimitations

Assumptions

The researcher assumed that because of limited resources, the organizations observed in this study did not have a professional in-house accounting staff to establish appropriate internal controls nor did they rely heavily on external accounting professionals. Additionally, the

researcher assumed the participants selected for the case studies were indeed small businesses as defined by having fewer than 100 employees.

Limitations

Some of the data in this study were self-reported, therefore, could not be independently verified. Because of this self-reporting, data could contain biases, such as exaggeration, selective memory, and attribution. To lessen this potential limitation, the researcher used multiple sources of collecting data, including an interview with the owner or his/her designee, direct observation, and documentation, from each small business to substantiate the accuracy of the data. Second, the results of this study could be limited if the researcher were restricted or denied access to certain documentation or personnel within the organization. To moderate the possibility of this limitation resulting from erroneous or incomplete data, the researcher endeavored to interview the owner or manager of each small business and the data were triangulated by using at least two different sources, including interview, direct observation, and documentation, to ensure a more thorough analysis (Yeasim & Rahman, 2012).

Delimitation

This study was used to explore the internal controls employed by small businesses. Therefore, only businesses with fewer than 100 employees located in Central Louisiana were included in the research study. Since non-profit organizations typically deal with issues that are different from for-profit organizations, such as the use of volunteers and the implementation of special or unique internal controls, non-profit organizations were not included in this study.

Significance of Study

This study is important in the field of accounting because it contributes to the accounting literature concerning internal controls, specifically, as related to small businesses. Also, this

study demonstrated several biblical truths, including the importance of being honest with God and each other. Van Duzer (2010) identified the primary purposes of businesses, which consist of providing goods and services that assist a community to grow and prosper. In addition, businesses provide employees with the opportunity to express their God-given uniqueness through meaningful and creative work. For a small business to fulfill these purposes, it must safeguard its assets through the implementation of effective internal controls in an effort to minimize the risk of employee fraud.

Reduction of Gaps in Business Practice

The significance of this study was the information obtained may help minimize the existing gap in the understanding of internal controls employed by small businesses. Researchers have not conducted many studies on the exploration of internal controls in small businesses and their impact on employee fraud risk. In fact, the Institute for Fraud Prevention cited only one study related to how ineffective internal controls in small businesses lead to higher levels of employee fraud risk in the United States since 2006 (Institute for Fraud Prevention, 2016).

Implications for Biblical Integration

Fraud is a not an accounting problem; it is a human problem. Fraud is stealing, taking something without permission. Leviticus 19:11 warns us to be ethical in our business dealing by stating: "You shall not steal; you shall not deal falsely; you shall not lie to one another."

Fraud usually occurs when the perpetrator thinks he/she has a need and rationalizes that he/she has a justifiable reason to steal. Some fraudsters justify their fraud by considering they are borrowing the money. However, Psalm 3:21 describes the person who borrows and does not repay "wicked" but "blessed" when he/she "eat[s] the fruit of the labor of [their] hands (Psalm

128:2). In Ephesians 4:28, Paul tells us "the thief must no longer steal. Instead, he must do honest work with his own hands, so that he has something to share with anyone in need." Unfortunately, some individuals do not have the education and/or experience needed to obtain the position and salary that their preferred lifestyle would require. Consequently, they resort to employee fraud.

Scripture warns us that we must be honest with God. Fraud is certainly not being honest with mankind or God. In Acts 5:1-11, Luke tells us about the deaths of Ananias and his wife, Sapphira. After they had sold a plot of land, they told Peter they had donated the proceeds to the church; however, they had not. Meyer (n.d.) wrote in his New Testament commentary that they "had selfishly embezzled the remainder for themselves" (para. 1). In addition, theologian John Stott (1994) wrote:

> Ananias and Sapphira were not so much misers as they were thieves. They wanted the credit and the prestige for sacrificial generosity, without the inconvenience of it. So, in order to gain a reputation to which they had no right, they told a brazen lie. Their motive in giving was not to relieve the poor, but to fatten their own ego. (para. 2)

Also, Verbruggen (2012) explained that Luke included this account in the scriptures because he wanted to tell us about "an unholy spirit," which is at work in the world (para. 5).

Although fraud cannot be completely eliminated, knowledge of internal controls can significantly reduce employee fraud risk. Most accountants are familiar with ways for identifying altered accounting data. Nevertheless, effectively fighting fraud involves taking a step further by understanding the human elements involved. This knowledge can help small businesses design internal control initiatives and identify where organizations are most at risk.

Relationship to Field of Study

Researchers have identified the characteristics of fraudsters; however, they have not determined the effectiveness of internal controls in mitigating employee fraud risk in small businesses. Internal controls serve a crucial role in the safeguarding of an organization's assets, which ultimately affects its fate. The results of this study may be used to assist small business owners and managers to become more knowledgeable of internal controls so they can be used to lower the potential for employee fraud risk.

A Review of the Professional and Academic Literature

The focus of this study was to explore the internal controls in select small business organizations in Central Louisiana in an effort to mitigate employee fraud risk. The problem addressed was that internal controls employed by small businesses are ineffective and lead to higher levels of employee fraud risk. It is important to have a more thorough understanding of general internal controls. Effective internal controls improve an organization's financial stability, create a competitive edge, and provides confidence to its owners. Therefore, the literature review includes a discussion on general internal controls, and specifically in small businesses. This discussion includes the five aspects of the COSO framework: control environment; risk assessment; control activities; information and communication; and monitoring. A thorough review of the COSO framework is essential to understanding the importance of internal controls and its role in mitigating employee fraud risk. Further, COSO addresses the unique challenges of internal controls faced by small businesses. The literature review distinguishes between fraud and unethical behavior, which is an important distinction as it relates to the exploration of internal controls. It also includes current literature on the

prevalence and consequences of employee fraud, which includes the evolution of fraud and fraud scandals.

Many fraud theories have been postulated in an attempt to better understand, identify, and minimize fraudulent activities. One such theory includes the fraud triangle, which serves as the most commonly used framework in fraud examination and is considered the foundation for forensic accounting. The fraud triangle explains that pressure, opportunity, and rationalization must be present for fraud to occur. Other theories to be discussed in the literature review are fraud diamond, which includes the element of capability, and fraud pentagon, which adds a fifth element, arrogance. In addition, another theory, the fraud scale, includes motives, conditions, possibilities, and realization. Finally, two other theories are described: triangle of fraud action, which includes the elements of the actual fraudulent acts, concealment and conversion; and the meta-model of fraud, which combines the fraud triangle and the triangle of fraud. These theories add to the understanding of fraud.

The literature review will discuss the characteristics of fraudsters, which provide insight into the study of the perpetrators. These characteristics, such as the organizational level of the employee, demographics (age), and personal risk profiles, will assist the reader in gaining a better understanding of the internal controls of small businesses and their impact on employee fraud. Literature on fraud prevention techniques, such as safeguarding assets and performing unscheduled reviews, will also be reviewed. Red flags, including extravagant lifestyles, family problems, and inaccuracies, were identified and their impact on employee fraud risk were reviewed.

Internal Controls

Business organizations must develop, implement, and review internal controls to better achieve organizational goals and decrease the risk of employee fraud. Verovska (2014) reasoned that the aim of effective internal controls is to improve its financial stability, create a competitive edge, and instill confidence in its shareholders. Oseifuah and Gyekye (2013) and Jahmani, Ansari, and Dowling (2014) defined internal controls as mechanisms developed to encourage employees to attain desired goals. Corns (1971) stated, "Controls protect weak people from temptation, strong people from opportunity, and innocent people from suspicion" (p. viii). Sun (2016) noted that weak internal controls can lead to errors in financial records, resulting in poor business decisions. Internal control is not a single event, as described by Dimitrijevic et al. (2015), but a series of activities that evaluate an organization's outcomes in comparison to its goals. Also, Ngwenya and Munyanyi (2015) defined internal controls as the compilation of procedures and policies that are created and implemented to foster efficiency, encourage accuracy in accounting procedures, and uphold laws and regulations. Ngwenya and Munyanyi (2015) further explained that internal controls govern both human and financial resources in an effort to monitor organizations to prevent fraudulent activities. Likewise, the International Standards of Auditing (2017) maintains that an internal control system refers to all policies and procedures adopted by an entity's management to achieve the organization's objectives in terms of safeguarding assets; detecting and preventing errors and fraud; and maintaining accurate and timely accounting records and financial information. In addition, the Committee of Sponsoring Organizations of the Treadway Commission (COSO; 2013) defined internal controls as the procedures directed by an organization's board of directors, management, and employees which have been established to promote realistic assurance concerning the achievement of

organizational objectives. The Commission explained that in essence, internal control involves everything that controls risks to an organization's operational efficiency and effectiveness, accurate financial reporting, and compliance with regulations and laws. The 2013 revisions of the original 1992 COSO integrated framework involved broad-based changes. D'Aquilo (2013) pointed out the framework that is now in place uses a principles-based approach. D'Aquilo described the 17 principles that provide clarity of the five components of the internal controls framework. D'Aquilo also explained the revised version stipulates all components should be operational, and internal controls principles across the five components should not result in any deficiencies. These principles, the author clarified, include important characteristics on which to focus. Further, D'Aquila (2013) emphasized that since organizational objectives, size, geographic regions, and type of industry differs from entity to entity, no two organizations should have the same internal controls. COSO deliberately used a broad definition of internal control to account for these differences (D'Aquila, 2013).

Pett et al. (2015) explained Principle 9 of COSO which declares that organizations should identify and assess changes that could significantly affect the entities' internal control system. Pett et al. provided examples of changes, such as new types of business transactions, new accounting standards, and important changes in business procedures, information and communications systems, and personnel that sustain control activities. These professional organizations emphasize the encompassment and importance of internal controls in business entities.

Organizations must continually be reassessing their internal controls and applying modifications necessary to maintain a minimum of fraud risk. Marais and Ostwalt (2016) noted that over 60% of the fraudsters indicated that weak internal controls lead to an opportunity to

commit fraud. Moreover, Morales, Gendron, and Guénin-Paracini (2014) emphasized that precise controls aid in overseeing two of the three prongs of the fraud triangle. Business organizations must take steps to determine potential employees' pressures by recognizing behavioral red flags and eliminating opportunities for employees to commit fraud.

Anti-fraud measures vary with regard to the type of fraud perpetrated. Two of the most common fraud methods used in small businesses, according to Kramer (2015), are billing and check tampering. In fact, Kramer reported that check tampering occurs three times more than in larger organizations. Other types of fraud include asset misappropriation, corruption and bribery, cybercrime, expense reimbursements, payroll, cash skimming (theft of cash prior to being recorded), cash larceny (theft of cash after it has been recorded), financial statement fraud, fraudulent disbursements, and procurement fraud (Hrncir & Metts, 2012; Phairas, 2016; Prasad, 2013; Steffee, 2014; Tschakert et al., 2016; Wells, 2004; Williams & Kollar, 2013). Indeed, Stone (2016) reported that cash larceny, skimming, and payroll fraud were reported twice as often in small businesses. Also, Elvin (2015) contended the type of fraud committed typically depends on the type of industry involved, such as scientific, technical, or professional. Elvin (2015) also disclosed the risk of fraud increased by 11% when organizations relied on online operations. Therefore, managers and owners should be aware of the most frequently used type of fraud occurring in their industry so they can establish internal controls specifically for those areas.

Procurement fraud is used in various industries. Bailey (2016), Hayes (2013), and Kramer (2015) detailed some ways that this type of fraud occurs. Sometimes fraudsters use fictitious vendors or shell companies to make payments for goods that have not been received; pay for and then return merchandise; make personal purchases; and use pass-through techniques,

which involve billing an employer for higher amounts than the actual goods or services rendered (Bailey, 2016; Hayes, 2013; Kramer, 2015). They also explained that small businesses are susceptible to being victims of forgery (e.g., endorsing checks and stealing company checks to pay for personal expenses).

Internal controls must be established that secure the procurement process. Bailey (2016) recommended that policies and procedures should be written. Bailey also suggested that employees should be routinely required to certify whether or not they have a conflict of interest with any vendors. Costs should be compared among vendors to identify rates that substantially exceed the average cost (Bailey, 2016). Then, Bailey pointed out that when variances have been identified, accountants should determine if a related-party relationship exists. Bailey (2016) also advised that managers should be aware if there have been extraordinarily large quantities of scrap and use of products because of faulty materials. These methods of internal controls should decrease the opportunity of procurement fraud.

Fraud can also occur during sales transactions. Bailey (2016) noted that selling services or products below market value, inflating the amount of sales to receive bonuses, extending unusual repayment terms or interest rates, and approving excessive sales allowances or returns and accounts receivable adjustments or write-offs are all examples of fraud that can occur with regard to sales. To avoid sales fraud, the Bailey (2016) recommends that guidelines must be established. Bailey then explains these transactions must be analyzed to compare price variations among customers to identify those who pay significantly below the average sales price. These internal control practices would decrease the opportunity of sales fraud.

In addition, Trompeter et al. (2013) specified details of the most common methods financial statement fraud occur. Trompeter et al. reported the most common technique used by

fraudsters was improperly recording revenue (61%), followed by overstatement of assets (51%) and understatement of liabilities and expenses (14%). Trompeter et al. also reported these techniques were also used in startup businesses which had little assets or revenue. Further, Mann (2013) highlighted that frequently collusion occurs which includes kickback schemes. Van Gent, Lindquist, and Smith (2013) cited examples of how fraud occurred in real fraud cases. Van Gent et al. (2013) noted the perpetrator opened a fictitious checking account using stolen personal information, such as a social security number, in which funds were wired by the fraudster who did not have to receive additional approval or review. Further, Nigrini and Mueller (2014) described how Mueller committed an $8 million fraud. Nigrini and Mueller (2014) explained that Mueller often logged on as someone else, made a request for payment, then logged on as himself and approved the payment. While it may originally appear that logging on as a different user is inconsequential, it can easily lead to fraud. In fact, the Computer Fraud and Abuse Act (CFAA) levies penalties on individuals who exceed authorized computer access to commit a fraud. In *United States v. Nasal* (*Nasal II*), the Ninth Circuit Court of Appeals upheld the conviction of a defendant who used someone else's login to commit fraud against a former employer. The court cited that only the system owner could grant authorization, not employees. Further, in *LVRC Holdings LLC v. Brekka*, the phrase "intentionally accesses a computer without authorization," as used in CFAA, was interpreted to mean that only the computer owner has the authority to allow access to its systems (Criminal Law, 2016, p. 1267). Therefore, a user does not have the right to log on as another person. Nigrini and Mueller (2014) also confirmed that part of Mueller's fraud scheme was to use business checks to pay personal bills that had a similar name to one of the businesses' creditors. Mueller created a vendor for which he created invoices and approved payment. Hall (2015) and Bailey (2016) confirmed that "related party" fraud,

which includes fake vendor and ghost employee schemes, are common ruses used among fraudsters. By studying fraudulent schemes perpetrated by convicted defalcators, business owners are more knowledgeable in establishing internal controls that minimize fraud risks.

With the growth of fraud perpetrators, business owners found it necessary to develop a model for evaluating internal controls. Biegelman and Bartow (2012) explained that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 as a voluntary organization. Professional finance and accounting organizations including Financial Executives International, the American Institute of Certified Professional Accountants, the American Accounting Association, the Institute of Internal Auditors, and the Institute of Management Accountants were involved in the formulation of COSO. In 1992, COSO constructed a model for assessing internal business controls. The five components of the model include factors in the following areas: control environment, risk assessment, control activities, information and communication, and monitoring (Cotton, Johnigan, & Givarz, 2016). These elements should be examined continuously and problems should be dealt with in a timely manner.

Control environment. Rae et al. (2017) noted the control environment forms the foundation for the other four components in COSO's model. Rae et al. added that all seven of the principles of the COSO report included aspects of integrity or moral guidance. Therefore, control environment may also be considered to be the ethical environment of an organization. Consequently, Wilkins and Haun (2014) underscored the first step in creating a strong control environment is for the owners to determine the organization's values, such as a commitment to excellence, integrity in working with stakeholders, and accountability. Wilkins and Haun (2014) emphasized the importance of owners and senior managers demonstrating these values to be role

models for their employees. Wilkins and Haun (2014) also recommended that the organization's control environment can be improved by developing a formal organizational structure, conducting background checks for prospective employees, providing written job descriptions, developing an employee code of conduct, and implementing a process for formal employee reviews. Henry (2016) reiterated that a controlled environment exhibits the importance of anti-fraud measures to an organization's employees. In addition, Laxman, Randles, and Nair (2014) expounded on each area. Laxman et al. explained that during the control environment, it is necessary to establish an anti-fraud organizational culture, create a positive work environment, and maintain an ethics hotline.

Anti-fraud culture. A number of studies have focused on the tone at the top in their research of the effect of organizational culture on frequency of fraud. Van der Wal, Graycar, and Kelly (2015) highlighted two schools of thought concerning employees' values. Van der Wal et al. explained that one philosophy is that moral standards are taught to children, and therefore, organizations are unable to influence individuals' conduct. Van der Wal et al. (2015) noted that scholars who believed in this viewpoint argued that organizations then could only rely on a hire and fire policy, in which good employees were hired and bad employees were fired. Another school of thought, according to the authors, is that organizations are, indeed, able to encourage the individual conduct of their employees. Therefore, management's idea shifted to the creation of management systems that involve organizational structure and culture. Murphy and Free (2016) and Wilkins and Haun (2014) described how the tone at the top is influenced by management's integrity, attitude, and ethical values. Murphy and Free (2016) and Wilkins and Haun (2014) clarified that when management encourages high ethical standards, the organization is less likely to be vulnerable to fraudulent activities. Johnson, Kuhn, Apostolou, and Hassell

(2013) referred to the mentality, ethics, or rationalization used to justify the act of fraud as fraud attitude. Johnson et al. also believed that attitudes such as dishonesty, low moral character, and lack of ethics were considered to be noteworthy fraud risk indicators. Tone at the top is defined by Patelli and Pedrini (2015) as an atmosphere created by owners, board of directors, or chief executive officers. Accordingly, they referred to the upper echelons theory proposed by Hambrick and Mason (1984), which identified that persons' in high positions of authority within an organization had a substantial impact on organizational practices. Further, Patelli and Pedrini (2015) explained the "trickle-down" theory, which explains that the leadership of the top echelon of an organization influences ethical conduct in the lower levels of the workplace. Gunz and Thorne (2015) pointed out the tone at the top influences all types and sizes of organizations. Gunz and Thorne (2015) also described two "unavoidable truths" concerning leadership and ethics: (a) ethical tone must be instituted at the top of the organization and communicated downward and (b) ethics must be reinforced by guidelines and actions of the organization, not just imposed by the organization (p. 1). The tone at the top creates an environment that encourages either integrity or unethical behavior.

An anti-fraud culture is also set by the "tone in the middle." Rae et al. (2017) stipulated the importance of middle management also setting the climate of the organization. Rae et al. explained that if middle managers are not committed to the ethics and values established by the company, it is immediately obvious to lower-level employees. Rae et al. also asserted that middle management understand the scope of the internal controls and their importance in achieving organizational objectives. In an organization, the ethics is only as strong as its weakest link. An entity's "tone at the top" must be translated into a proper "tone in the middle" before it can reach the rest of the organization.

Positive work environment. It is important to create a positive work environment. Biegelman and Bartow (2012) described several factors that can create a negative atmosphere, thereby increasing fraud risk. Biegelman and Bartow (2012) provided examples of factors to avoid, such as not being recognized for job performance, poor compensation, lack of well-defined organizational responsibilities, inadequate training and advancement opportunities, and poor communication. In addition, Jahmani and Dowling (2015) acknowledged the importance of positive employee treatment. Guo, Huang, Zhang, and Zhou (2016) asserted the significance of adhering to the human capital theory which argues that fair treatment of employees enhances the ability to hire the best skilled workers, reduce employee turnover, and motivate managers to make the greatest human capital investments. Guo et al. posited that organizations with better employee-friendly policies are less likely to have ineffective internal controls because the workers will be more motivated to ensure the entities' success. Moreover, Balsam, Jiang, and Lu (2014) and Rice, Weber, and Wu (2015) examined how managers' salaries related to the effectiveness of internal controls. Managers may be encouraged to strive for effective internal controls because unfavorable mechanisms will negatively affect the organization and may possibly result in reduced salaries or a reduction in force (Balsam et al., 2014; Rice et al., 2015). Therefore, one of the most important aspects of establishing a positive control environment is to create a positive work environment for all employees regardless of their position in the organization.

Hotline. Organizations that use hotlines significantly reduce losses due to fraud. The ACFE *Report to the Nations* (2016) found the use of hotlines was the most common method that fraud was detected. Yet, the report cited only 18% of small businesses implemented hotlines, whereas 82% of large organizations had one. The report also indicated 40% of the fraud tips

received were made from nonemployees, such as customers and suppliers. In addition, ACFE reported that organizations that had hotlines had fewer losses than those without this anonymous, confidential tool. Zhang, Pany, and Reckers (2013) argued the anonymous hotlines strengthened internal controls. They explained the goal in providing hotlines is to decrease the tipster's hesitation to become involved in the situation.

Hotlines are not just used to report suspected fraud. Biegelman and Bartow (2012) recommended they also be used to inquire about appropriate business policies and clarify proper procedures. Therefore, the authors suggested that businesses may want to call their mechanism by a different name that would be less negative and more inclusive. Samuels and Pope (2014) reported that in a survey conducted by the Ethical Leadership Group, lines that were called "Hotline" or "Alert Line" only received four calls per 1,000 employees whereas reporting mechanisms called "Help Line" or "Open Line" received 23 calls per 1,000 employees. Although it may appear to be a matter of semantics, there is an important distinction in most employees' minds. Hotline or Alert Line gives the impression it is an emergency, similar to a 9-1-1 call, whereas Help Line or Open Line implies the notion they are providing a mentoring service. Samuels and Pope (2014) recommended the hotline be available 24 hours a day since their research indicated 40% of the tips were received outside of regular business hours. Moreover, Zhang et al. (2013) noted, in 2007, the Ethics Resource Center reported 56% of employees acknowledged they had observed misconduct, yet only 63% of those observers reported it. Regardless of the name of the system used for employees to report fraud tips, hotlines are an important part of an internal control system.

Some individuals may be reluctant to make claims of fraud because they fear retribution.

Whistleblowing is defined by Lee and Fargher (2013) as "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (pp. 284-285). For government agencies and contractors, healthcare providers, and any organization that receives government funds, whistleblowers or tipsters do not have to fear negative consequences because of the False Claims Act. Biegelman and Bartow (2012) indicated the original False Claims Act was passed in 1863 after Congress discovered occurrences of fraud in the Union army that resulted in defective weaponry. At the time, the authors explained, the law was not used often because of government-issued reductions in the monetary amounts that the plaintiffs could receive. However, Biegelman and Bartow (2012) described the 1986 amendments to the act which provide whistleblowers an increased amount of recovered proceeds when they related information concerning government contracts. Further, Biegelman and Bartow (2012) explained the revised False Claims Act has been expanded through new legislation, including the Dodd-Frank Act, the Affordable Health Care Act of 2010, and the Fraud Enforcement and Recovery Act of 2009. Legislation has made it more conducive for whistleblowers to relate their suspicions of fraud to authorities.

The majority of employees work for organizations that do not receive government funds and therefore are not protected by the False Claims Act. These employees may find it difficult to report wrongdoing for fear of retaliation. Gao, Greenberg, and Wong-On-Wing (2015) reported that younger employees or those in lower positions in the organizational hierarchy typically do not feel comfortable reporting the misconduct of more experienced, higher-level managers. Because of the wrongdoer power status syndrome, Lee and Fargher (2013) recommend that organizations create a climate that targets lower-level employees for training in how to report

their concerns for possible fraud. In addition, Latané and Darley (1968) described the bystander effect. Latané and Darley (1968) explained when several people are witnesses of a situation, it is less likely for an individual to report the incident than when only one individual observes the act. A single observer feels less personal responsibility and since they share the cost of nonintervention, it is less likely to convey any wrongdoing (Latané & Darley, 1968).

The ease and availability to use hotlines to report potential fraudulent activities are also important. In addition to fearing retribution, employees are typically more comfortable trusting members within their own group. Burt (2016) explained this philosophy, the social identity theory (SIT), should be recognized when creating employee hotlines. Otherwise employees may consciously decide to withhold relevant information because they are concerned with the possible negative influence on the organization (Burt, 2016). Organizational silence can be detrimental to an organization. In the case of reporting prospective fraud, employee silence can result in a negative public image or even bankruptcy (Burt, 2016).

Risk assessment. Regardless of the size of the organization or whether it is private or public, all entities face both internal and external risks. Frazier (2016) explained that prior to risk assessment, organizational objectives must be determined. Frazier (2016) clarified that risks can be identified and analyzed in accordance with the goals. It is important to assess fraud potential and determine appropriate means to respond to significant fraud risk. Power (2013) pointed out that fraud risk focuses on internal control systems, risk, and managerial responsibility. Power (2013) argued that current fraud risk management focuses on prevention techniques rather than the historical concern with ascribing responsibility and assigning retribution. In essence, risk assessment concerns an organization's future, which is managed in

the present (Power, 2013). Wilkins and Haun (2014) emphasized that fraud assessment is not only concerned with minimizing risks, but managing them.

Joseph Wells (2011), the founder of Association of Certified Fraud Examiners (ACFE), asserted that fraud was a problem that required effective internal controls and surveillance of employees within an organization. In addition, PricewaterhouseCoopers (PwC; 2016) concluded that 22% of the organizations surveyed had not conducted any fraud risk assessments in the two years prior to the study. PwC also found that 67% of the chief executives reported more threats to the growth of their businesses as opposed to 59% in 2015. This organization pointed out a problematic trend—that due to a lack of internal controls, fraud is frequently left to chance. PwC stated that "the burden of preventing, protecting and responding to economic crime rests firmly with organizations themselves" (p. 8). PwC summarized the importance of assessing fraud risk by stating: "To be forewarned is to be forearmed for success" (p. 12). In addition, Marais and Ostwalt (2016) expounded on the idea that organizations should conduct regular risk assessments because the type of fraud threats are continuously changing. Rose, Sarjoo, and Bennett (2015) explained the 2013 update of COSO's *Internal Control-Integrated Framework* recommends that organizations conduct routine fraud risk assessments as part of the overall risk assessment. Rose et al. further elaborated that Principle 8, which focuses on fraud, describes four areas that should be evaluated: fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, and illegal acts. Recognizing inherent fraud risks enables an organization to understand its vulnerability while evaluating the effectiveness of internal controls to aid an enterprise to comprehend its current level of risk exposure.

Wilkins and Haun (2014) reiterated there are four areas that should be evaluated in risk assessment, according to COSO: financial, strategic, operational, and compliance. Wilkins and

Haun (2014) explained that after identifying the risks, they should be prioritized by their significance, in terms of dollars and likelihood, the probability of occurrence. The authors then explained the next step is to develop a response to the risk. Organizations may choose to either reduce, accept, share, control, or avoid potential risk (Wilkins & Haun, 2014). After the risks have been prioritized, managers should develop responses to the top three or four risks.

Control activities. Wilkins and Haun (2014) defined control activities as actions delineated through policies so that organizational objectives can be achieved by mitigating risks. Further, Henry (2016) contended that control activities associated with fraud prevention can be manifested in the hiring, onboarding, and training process, in addition to the organization's policies and procedures. Managers should implement and design anti-fraud methods by evaluating current controls and establishing new ones to reduce the risk of fraud.

Background checks. Past performance is a good indicator of future performance. Preemptive actions begin with prescreening job applicants by validating work experience and education, conducting criminal background checks, and performing credit checks (Marquet, 2017; Young, 2014). Approximately half of victim organizations ran a background check at the time the perpetrator was hired, according to ACFE (2016). In 11% of cases, the background check revealed at least one red flag, such as prior criminal activity, employment issues, or financial problems. Biegelman and Bartow (2012), Brody, Perri, and Van Buren (2015), and Glodstein (2015) reported the following components that a background check might include: employment history, including nature and length of service; education and professional licenses; personal references; criminal and credit history; medical history; and use of social media.

Typically, employers confirm prospective employees' employment history. Brody et al. (2015) recommended that employers not only confirm the nature and length of service for the

applicant, but also specifically ask former employers if they would re-hire the individual. Brody et al. cited several examples of cases in which employees who were previously fired for ethical concerns were hired in new organizations, only to repeat their unethical behaviors. Employers conduct honesty and integrity assessments as well as verifying previous work experience (Brody et al., 2015). Brody et al. contended these evaluations, in which applicants are posed ethical concerns, may be indicative of impending behaviors. These assessments may produce false negatives or positives and might be a violation of privacy (Brody et al., 2015). Although this is an area which needs further study, the use of honesty and integrity assessments should be researched because employers are legally liable for many of their employees' actions. Therefore, employers must utilize all means possible to make the best employment decisions.

The U.S. Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) prepared a joint publication to aid employers in conducting background checks on prospective employees. The report indicates it is not illegal for employers to require background checks or ask questions concerning these topics, with the exception of certain medical topics. However, employers must be careful to comply with federal laws that protect prospective employees from discrimination. The EEOC includes discrimination based on religion; sex; color; race; national origin disability; genetic information, which includes family medical history; and age, which includes individuals 40 years or older. Also, all background checks must be in compliance with the Fair Credit Reporting Act (FCRA), which is enforced by the FTC (Background checks: What employers need to know, 2014).

Although it is wise to conduct background checks for potential employees, employers must perform due diligence because there could be extenuating circumstances for some situations, such as a high credit card history. In fact, Tonowski (2015) indicated there has been a

decrease in the use of credit history in employment screening. Tonowski also pointed out that according to the FTC, applicants must not only be notified that information gathered in a background check might be used in employment decisions, but employers must also obtain written permission from prospective employees to conduct such an investigation. Tonowski (2015) illustrated the importance of following EEOC regulations by citing several court cases in which violators settled out of court for millions of dollars. It is helpful for employers to conduct employment screening; however, they must be in compliance with EEOC and FTC regulations.

The use of criminal history in a background check continues to be a concern. Tonowski (2015) asserted that many human resource managers suggest that criminal histories should be considered further in the hiring process. Federal law currently does not prohibit employers from asking prospective employees about their criminal history; however, the EEOC laws do not allow employers to make hiring decisions that may be in violation of Title VII of the Civil Rights Act of 1964 (Tonowski, 2015).

Manager or owner review. According the ACFE (2016), manager or owner review of bank accounts, expense reimbursements, and petty cash was the second most common method used to detect fraud schemes. In addition, Neguriţă and Ionescu (2016) recommended that managers adequately supervise employees who are responsible for assets, particularly those items in which the owner cannot be easily identified, which can be easily sold, and which are located further away from the main site. Further, Kapp and Heslop (2015) suggested receipt books be numbered chronologically and reviewed to determine that no receipts have been removed or voided. They also recommended that managers or owners should ensure that accounting and source documents have been linked together.

Job rotation and mandatory vacations. Only about 20% of the organizations surveyed by the ACFE (2016) used job rotation and mandatory vacations as an internal control. Kapp and Heslop (2015) recommended that duties should be rotated periodically to make fraud concealment more difficult. They described several instances in which fraudsters were caught because they refused to take vacations or went to work during difficult circumstances, such as returning to work soon after a surgical procedure. Likewise, Neguriţă and Ionescu (2016) argued the importance of requiring mandatory vacations for employees who are in positions of significant control.

Separation of duties. There should be a separation of job duties to avoid one employee having too much authority. Kitching, Pevner, and Stephens (2013) and Neguriţă and Ionescu (2016) recommended there should be separation of duties between employees performing information technology, accounting, and operating activities. Also, job duties should be segregated. If only one or two people are involved in the accounting process, then Hrncir and Metts (2012) and Verick (2013) recommended the owner should be actively involved by knowing the intricacies of the organization's revenue and expenses. Owners should establish their own responsibilities and make employees aware of those duties (McCole, 2014). Further, Ngwenya and Munyanyi (2015) and Howard (2015) elaborated that effective segregation should mean that one individual is never in a position to be responsible for initiating, approving, and recording a transaction. The authors explained that cash should not be in the same location as the recordkeeping. Klein (2015) pointed out that employees should not have unlimited authority of any transaction or accounting function. Glodstein (2009) declared that checks should require two signatures, and one person should not be responsible for both human resources and financial

records. Internal controls should prevent employees from performing more than one function of a business transaction.

Surprise audits. Although the ACFE report indicates that surprise audits are one of the least anti-fraud controls methods used, Murphy and Free (2016) noted it is one of the best ways to reduce the loss due to fraud. Further, Camilo and Grimaldos (2014) argued that independence is a necessity when conducting objective audits.

Information and communication. It is essential to maintain effective information and communication with employees. Frazier (2016) emphasized the importance of communicating timely information in appropriate forms so that employees can perform their responsibilities appropriately. He stressed that all employees must have the means and ability to communicate up, down, and across the levels of an organization. Also, the author reiterated the importance of all employees understanding their role in the internal control system. Pett et al. (2015) explained that Principle 13 of COSO emphasized the importance of organizations generating and using pertinent information to support the effectiveness of internal controls. They pointed out that since organizations depend on having reliable information, they must assess changes in the information system to ensure the execution of control activities. In addition, McNeal (2016) pointed out that active communication with employees creates an open-door policy and culture of trust which are beneficial to the organization. This formal policy, she explained, should state that employees are encouraged to bring concerns to management and all managers at all levels of the organization have the responsibility to be accessible and open to discussions with employees. The author also discussed the importance of including an organizational chart with the explanation the employee's direct supervisor should be the first person to go to with a concern; however, the policy should also allow employees to take apprehensions to other levels or to

human resources. Oseifuah and Gyekye (2013) explained that information is the means by which employees are made aware of internal controls and management's commitment to an anti-fraud climate. They pointed out that information and communication connects all elements of the COSO framework. Deliberate fraud training is the best way to communicate with employees.

Employee training. One of the most important ways to be proactive is to train employees on why fraud occurs, red flags to look for, and how to report any concerns. Oseifuah and Gyekye (2013) asserted that employees must understand their role in the internal control system and how their individual duties relate to the work of other people. In addition, Biegelman and Bartow (2012) suggested that training should include discussions of the fraud risk, the types of fraud that could be perpetrated against the company, what can be done to stop fraudulent acts, and how fraud impacts both the business and employees' lives. They pointed out that a well-designed reporting system will fail without employee training. The authors recommended that fraud awareness education has four parts: definition of fraud, the negative effect fraud has on organizational profits, examples of various types of fraud, and what to do if employees suspect fraud. Beauprie (2015) also recommended that employees should be informed of the financial authority process. Further, he specified that employers should warn employees of the risk of using social media websites. It is essential, according to Simha and Satyanarayan (2016), that all employees accept responsibility for detecting fraud occurrences. While the connotation of occupational fraud usually implies that the employee is the recipient of the funds, employees could also be manipulated to commit fraudulent acts that would benefit other people. For example, the author explained that during fraud training, employees should be made aware of "Fake President" schemes in which fraudsters assume the identity of authentic vendors or

organizational executives who request that funds be sent to new accounts. Anti-fraud training is not only beneficial, but essential, for a successful fraud awareness and prevention program.

Written code of conduct. It cannot be assumed that all employees will know what is expected of them. A code of conduct, which includes an explanation of the organization's values that are based on honesty and integrity, should be included in the employee manual or as a separate document as well as emphasized in employee training seminars. To this end, McNeal (2016) emphasized that all personnel manuals should include the organization's mission statement and its core values. She also recommended that all company policies and practices should be made with the mission statement in mind. Henry (2016) emphasized that a written code of conduct equips employees with the knowledge of the ethical values of the organization, the skills necessary to detect fraud, and the training about the actions to take when fraud is alleged. In addition, Ebberts (2015) noted the Ethics Research Center, a non-profit research organization based in Virginia that is devoted to the advancement of high ethical standards and practices, found ethics awareness was an invaluable asset to businesses. In fact, the author documented that observed misconduct increased from 55% to 83% for those organizations that did not have a strong ethics program. Biegelman and Bartow (2012) recommended it is helpful for these values to be included in routine performance evaluations to indicate how the employee contributed to the work environment.

Monitoring. Surveillance is an important aspect in preventing fraud. Wilkins and Haun (2014) defined monitoring as performing assessments to determine if the five components of internal controls are present and operational. Levy (2016) and McCole (2014) noted the most effective control in small businesses is owner/manager supervision because fraud risk is reduced when employees know they are being watched. Likewise, Goldstein (2015) emphasized that

employees need to be aware of the internal controls. He also suggested that organizations need to prevent employees from having access to both accounting records and physical resources. The monitoring of internal controls should be on-going.

Managers should take advantage of utilizing technology to aid in monitoring activities (Laxman et al., 2014). Beach and Schiefellxin (2014) detailed the importance of using technology to monitor unstructured data. Oftentimes they explained fraud schemes can be discovered through such unconventional means as email, Internet logs, telephone calls, text messages, and social media messages. Unfortunately, many organizations fear jeopardizing employees' privacy so they avoid technology that can assist in monitoring these types of unstructured data. The authors recommend seeking legal counsel before instituting such a policy, but most issues can be avoided if the policies are explained in the personnel manual. Organizations must determine if the benefits of data monitoring exceeds the costs.

Internal Controls in Small Businesses

The definition of small business organizations varies from country to country. Oseifuah and Gyekye (2013) explained that various definitions are based on the number of employees, turnover rate, gross assets, and amount of investments. However, they explained the most common differentiation is based on the number of employees.

COSO designed its 2013 internal control framework around the unique challenges faced by small business organizations. Specifically, Rittenberg (2006) explained that many small businesses find it difficult to segregate job duties, recruit an auditing professional, utilize extensive documentation, and use appropriate information technology to make assumptions about the quality of internal controls. Further, the author suggested that while many small

businesses have effective internal controls over financial reporting, they may face challenges in other areas, such as segregation of duties.

Many small businesses are victims of fraud simply because they have some misconceptions concerning fraud. Some common mistaken beliefs include the idea that their organizations are too small to be targeted by fraudsters; all of their employees are loyal, like family members; they have complete control of their businesses; they do not need internal controls; and fraud would not cost their business very much (Fountain, 2014; Gagliardi, 2014; Kennedy & Benson, 2016; Loria, 2015). In addition to having some mistaken beliefs regarding fraud, small businesses also sometimes find it challenging to institute effective internal controls. For example, Glodstein (2015), Klein (2015), and Stone (2016) described the challenges small business organizations may have concerning separation of duties. They insisted that one individual should not have authority or responsibility over more than one part of a transaction. In addition, the authors explained the importance of business owners being active in the accounting functions. Glodstein (2015) recommended that owners regularly review accounting documents, such as bank statements, cancelled checks, payroll expense reports, and cash receipts and disbursements. Stone (2016) and Verick (2013) also suggested that small business organizations invest in software which will streamline accounting functions and provide additional security. Stone (2016) and Verick (2013) recommended the software purchased should combine functionality, provide owners with information on business performance, enable owners and managers the ability to select security features, and focus on actions prioritized by risk. Also, Stone (2016) and Verick (2013) indicated the importance of not overwhelming employees by being able to gradually implement its use in a phased manner. Newman and Neier (2014) reiterated the importance of using technology to analyze data to identify potential

employee misconduct. Also, Fountain (2014) explained that small business owners must be proactive in their approach to identify unauthorized transactions that pass through their computers' firewalls. Fraud will continue to evolve as technology advances. Small business owners must continue to be vigilant in their use of internal controls in an effort to reduce their level of employee fraud risk.

While technology can be advantageous to use in small businesses, it can also be used to commit fraud. Gilmore-Allen (2015) described how small organizations can be victimized as a result of technology-related frauds, such as data breaches, hacking attacks, and identity theft. Gilmore-Allen (2015) also sited incidents where these organizations are victims of phishing emails because they may not have procedures against employees responding to the message. Since small business entities do not have the same protection that individuals have, they must perform risk assessment, specifically for potential fraud with regard to technology (Gilmore-Allen, 2015). The author suggested that organizations need privacy and security policies concerning the use of strong passwords, social media, email, and routine password changes. Gilmore-Allen (2015) emphasized the importance of including safeguards to avoid technology fraud in their employee training. Business owners must remain diligent in reviewing financial records because even the most trusted employee could be capable of fraud. Although there are a number of internal controls available, each small business must select and utilize the most appropriate internal controls for the organization.

Employee Fraud

At first glance, it may appear there is a simple definition of employee fraud. However, one of the first things a researcher must do is to acknowledge and understand the difference between fraud and unethical behavior. Therefore, Anand, Dacin, and Murphy (2015) and

Louwers, Ramsay, Sinason, Strawser, and Thibodeau (2015) noted that different definitions of fraud and distinctions between unethical versus ethical behavior vary among different individuals, organizations, and societies. In addition, Anand et al. (2015) and Louwers et al. (2015) pointed out that fraud can be conducted by individuals as well as groups of people. To further complicate matters, the Association of Certified Fraud Examiners (2016) recognized 44 different types of fraud schemes that have been enacted within organizations. Also, fraud is defined differently if it in a civil or criminal case. Waite (2013) explained that in the United States and Canada, the standards of proof of fraud is significantly higher in criminal charges than in civil cases. In *Southern Development Co. v Silva*, 125 U.S. 247 (1888), the ruling was made that determined a civil fraud is committed only if the perpetrator knowingly falsified information that resulted in a loss for the other party. Therefore, in the United States, organizations must determine if sufficient evidence is present to make criminal charges or if it would be more advantageous to seek civil remedies.

Prevalence of Employee Fraud

Fraud is not a new phenomenon. It dates back to Antiquity as people have used trickery, deceit, and manipulation to gain land or money in an effort to make a profit. Petraşcu and Tieanu (2014) described the evolution of the field of audit as a means to detect fraud. Archaeologists have found evidence of the existence of rudimentary forms of accounting and the verification of accounts in ancient Babylon and Egypt (Petrascu & Tieanu, 2014). Further, Petrascu and Tieanu highlighted as commercial trade increased, recordkeeping practices as well as fraud increased. Consequently, Luca Paciolo, the founder of accounting, created the double-entry bookkeeping system in the late 15th century to decrease the probability of misrepresentation of financial information and theft. Petraşcu and Tieanu (2014) pointed out that this method was

the foundation of not only our current method of accounting, but also gave us the ability to increase the ability to audit accounting records to detect fraudulent schemes.

Since 1998, *The Accounting Degree Review* (2016) has identified 10 of the worst corporate accounting scandals that have taken place in the United States. They indicated that scandals, including Enron, Worldcom, and Healthsouth, cost investors and shareholders nearly $369 billion as well as inflated assets and sales by approximately $13 billion. In addition, Gerard and Weber (2016) detailed the Koss Corporation fraud totaling over $30 million, which resulted in a negative impact on employees and shareholders and a decline in stock price from over $25 per share in 2006 to $5 per share after the discovery of the fraud in 2009. Unfortunately, fraud in not limited to the United States. Abdel-Khalik (2014) listed the top 14 worldwide cases in which the loss exceeded $200 million per case. In fact, Adbel-Khalik found that direct losses in these cases exceeded $43 billion. Reports of such organizational scandals have brought the subject of fraud to the forefront. Prior to these events, Levy (2015) asserted that "auditors treated fraud not as something to search for, but rather as something to deal with, if they stumble upon it" (p. 6). Fraud not only affects large corporations, but small businesses as well. Although the total amount of fraud is certainly much greater in large organizations, small businesses are disproportionately victimized. In fact, many small businesses actually dissolve as a result of the impact fraud has on the organization. Fraudulent activities affect all business relationships and employee morale. This action, in turn, affects the local economy (ACFE, 2016; Petraşcu & Tieanu, 2014). Therefore, it is essential that internal controls in small businesses and potential red flags be explored to ascertain their impact on employee fraud risk.

Consequences of Fraud

Employee fraud causes significant financial losses to victim organizations. ACFE (2016) indicated the total loss in the 2,410 cases studied exceeded $6.3 billion. Moreover, Verschoor (2014) anticipated the cost of fraud in business organizations will continue to rise. Fraud has significant negative impact on both the perpetrator and the organization. Galletta (2015) clarified that with the extensive use of social media, the effects of fraud on business organizations can be devastating. In addition, Galletta explained the consequences are immediate because of the speed in which a report can "go viral." Once an organization gains a negative image after fraud has been discovered, the business then must determine the best method to address the adverse reputation. Benoit's (1997) typology best explained the five methods owners and managers can utilize to restore an organization's image: denial, evasion, reduction, mortification, and correction. Erickson, Lukes, and Weber (2014) asserted that denial can be a simple denial or shifting the blame. They further acknowledged that evasion of responsibility includes such actions as claiming the action was accidental; scapegoating or blaming the activity on someone else; defeasibility or lacking the knowledge to act appropriately; or claiming the organization had honorable intentions. Erickson et al. also explained that reducing the offensive act refers to minimizing the problem, offering compensation for losses, or reducing the credibility of the accuser. Moreover, the Erickson et al. described mortification as admitting guilt and apologizing. Taking corrective action is the most responsible act for the organization to take because the owners or managers take steps to prevent a reoccurrence of the activity (Erickson et al., 2014). Regardless of the means taken, it is imperative that organizations take action to improve their less than stellar image.

Study of Fraud

Fraud has been studied throughout many disciplines to better understand its nature and the best methods to foster prevention and detection programs. These studies have developed into the following theories: fraud triangle, fraud diamond, fraud pentagon, and fraud scale. Researchers have also developed a theory that explains all of the aspects a perpetrator must go through to successfully commit fraud, which is called the triangle of fraud action. Still other researchers encompass all of the elements into the meta-model of fraud.

The fraud triangle. Understanding why people commit fraud is one of the first steps in preventing it. Worldwide professional auditing organizations, academic textbooks, and fraud examinations use the fraud triangle as the foundation for forensic accounting. In fact, Free (2015) explained the fraud triangle is the most commonly used framework in fraud examination in the United States, Australia, United Kingdom, Hong Kong, and Lebanon. He clarified that although the fraud triangle is credited to Donald Cressey from his 1953 research, the actual term was not coined until Steve Albrecht first used it several decades later. Albrecht began his research by adapting the concept of fraud from solely a criminology standpoint to an accounting context. Next, he identified 82 different fraud-related variables, which he separated into three categories that he labeled situational pressures, opportunities to commit fraud, and personal integrity (Simha & Satyanarayan, 2016). Prabowo (2016), Rodgers, Söderbom, and Guiral (2015), and Schuchter and Levi (2015) explained the fraud triangle is a heuristic framework which explains that three elements must be present for an act of fraud or trust violation to be committed. Prabowo (2016), Rodgers et al. (2015), and Schuchter and Levi (2015) indicated that a fraudster must perceive a need or have an incentive or pressure, an opportunity to perpetuate the fraud, and then rationalize the notion that committing the fraud is worth the risk. Further,

Dellaportas (2013) and Ruankaew (2016) pointed out that pressure can occur in all employees at any point during their employment. Dellaportas (2013) and Ruankaew (2016) also emphasized the pressure does not have to be real, but it is typically a response to economic pressures, such as living beyond one's means, financial losses and increased debt, and even greed. In fact, Albrecht, Hill, and Albrecht (2006) found that approximately 95% of fraud instances were caused by financial pressures. Also, Mackevičius and Girūnas (2013) described the three types of pressures as being personal financial incentives to live a higher lifestyle, pressure from one's employer to meet the interests of the organization, and external pressures. According to Van Gent et al. (2013), fraudsters usually steal for immediate use rather than to establish secure financial futures. Regardless of the reason, fraud is a serious problem for all businesses.

In an attempt to explain the reasons people commit fraud, Wells, Kranacher, and Riley (2011) first presented Professor Jason Thomas' M.I.C.E. model. In this model, Thomas used the acronym MICE to represent four types of incentives to a prospective fraudster: money, ideology, coercion, and ego/entitlement. Ruankaew (2016) reiterated the importance of fraudsters not viewing their actions as unethical and illegal. Perpetrators must rationalize their action before a fraudulent act can occur. Simha and Satyanarayan (2016) explained that rationalization is the most challenging aspect of the fraud triangle for employers or auditors to assess. Ruankaew (2016) explained although employers cannot control the perceived pressure and rationalization that a person experiences, they do have control over the opportunity for an employee to commit the fraud. Therefore, it is imperative for business managers and owners to determine ways to reduce the opportunity for fraud.

The fraud diamond. Notwithstanding the popularity of the fraud triangle, there has been some criticism. Consequently, several additional models have been developed which

augmented the original design. These new designs attempted to identify additional factors that must be present for fraudulent behavior to occur. For example, in 2004, Wolfe and Hermanson developed the fraud diamond which added capability, a fourth dimension. They argued that even though the three elements of the fraud triangle were present, perpetrators must have the ability and skills necessary to commit the fraud. Therefore, capability is listed as the fourth element in the fraud diamond. Wolfe and Hermanson (2004) determined that perpetrators must be in a position of authority within the organization to have the intelligence of the organization's accounting and internal controls to exploit the business' weaknesses. Fraudsters must also possess the ability to manipulate the victim into incorrectly believing that the perpetrator can be trusted, thus creating a false sense of security. In addition, fraudsters must be able to handle the stress involved with the threat of getting caught and possess the confidence that the fraud will remain undetected (Abdullahi & Mansor, 2015; Dilla, Harrison, Mennacke, & Janvrin, 2013; Mihret, 2014; Wolfe & Hermanson, 2004). Mackevičius and Girūnas (2013) and Yusof et al. (2015) posited that the fourth element, capability, is particularly important in long-term fraud cases. The fraud diamond theory emphasizes the importance of recognizing an employee's capability to commit fraud so that organizations can find solutions to decrease this behavior.

The fraud pentagon. The Crowe fraud pentagon is another transformation of the fraud triangle. This model was developed by Jonathan Marks, a partner in Crowe Horwath who served as a leader of the Fraud, Ethics, and Anti-corruption Product and Solutions initiative. In the fraud pentagon, the five elements are pressure, opportunity, rationalization, arrogance or lack of conscience, and competence or the power for an employee to perform fraudulent acts (Free, 2015; Playing offence in a high-risk environment, n.d; Yusof et al., 2015). The authors explained that the element of arrogance refers to an attitude of entitlement and superiority. They

described competence as elaborating on the fraud triangle's element of opportunity to include the perpetrator's ability to take advantage of circumstances and bypass internal controls. Arrogance and competence play major roles in determining if an employee has the ability to commit fraud.

The fraud scale. The fraud diamond also has some drawbacks; namely, it does not take into account the role of internal controls nor when there is the greatest risk for fraud. Therefore, the fraud scale was developed. Mackevičius and Girūnas (2013) included the elements of motives, conditions, possibilities, and realization in the fraud scale. They explained that all of these components are related to internal controls. Generally, motive refers to a fraudster's pressure or incentive to commit fraud. The authors clarified that some of the conditions or circumstances necessary for fraud to occur include the competence and honesty of the organization's managers; structure and financial status of the company; and the activities, accounting, and internal controls of the organization. They described that another component of the fraud scale, possibilities, is affected by the perpetrator's position in the company, access to organizational accounting records and assets, and knowledge of internal controls. The authors contended that the element of realization is a more apt term than rationalization because realization includes the fraudster's personal characteristics, such as integrity, that allows him to objectively evaluate his willingness to commit the fraud rather than only justifying the crime. The authors clarified that the fraud scale can be used to determine the level of fraud risk. A study of the components of the fraud scale will assist scholars, researchers, and auditors to study fraud approaches and be able to estimate the level of fraud risk.

Triangle of fraud action. Although the fraud cycle begins with the fraud triangle, Steven Albrecht is attributed to the development of the triangle of fraud action (Albrecht et al., 2012). McMahon et al. (2016) and Trompeter et al. (2013) explained the elements of the

fraudulent act, concealment, and conversion in a model called the triangle of fraud action. Further, Mihret (2014) emphasized that by providing evidence of how the fraud was perpetuated, concealed, and then converted to a usable form for the fraudster, the perpetrator is less likely to deny his or her role in the fraud. In other words, the triangle of fraud action provides an analysis of the pre-fraud situation and the post-fraud aspects of the crime. It is important for small business owners to realize that not only should they be aware of the opportunities of fraud they must control, but they must also be able to look for evidence of any fraudulent acts and how the crime could be concealed to develop comprehensive internal controls.

Meta-model of fraud. The fraud triangle and the triangle of fraud action are combined to form a comprehensive meta-model of fraud that relates a potential fraudster's internal perceptions to the actions necessary to complete the fraud successfully. Dorminey et al. (2012) reinforced the idea that use of the meta-model assists fraud prevention specialists understand how to prevent, deter, detect, and investigate fraud in a more complete manner. Dorminey et al. pointed out that Cressey's fraud triangle represents the pre-fraud perceptions of the potential fraudster whereas Albrecht's post-fraud triangle of fraud action signifies the issues that lie between the potential perpetrator and the financial reward of the criminal act. Trompeter et al. (2014) explained that between the fraud triangle and the elements of fraud lies the anti-fraud measures. Trompeter et al. reported that examples of these organizational and societal interventions include internal controls, corporate regulations, legal and ethical concerns which are aimed at minimizing the number and impact of fraudulent acts. These interventions have been identified as prevention, deterrence, and detection (Trompeter et al.). Although these interventions are not within the perpetrator's control, they influence the fraudster's judgment of the probability of committing a fraud successfully (Trompeter et al., 2014). By using the meta-

model, researchers, managers, and business owners can conduct a more comprehensive analysis of the elements of fraud.

Additional fraud theories. In addition to the traditional fraud theories described above, Biegelman and Bartow (2012) have developed additional philosophies based upon observation. The authors clarified that although the following theories may appear humorous at first, they accurately describe why and how fraud is committed:

Tip of the iceberg theory. The presumption in this theory is that often when a fraud is detected, it is only a small portion of the entire fraudulent activities (Biegelman & Bartow, 2012).

Potato chip theory. The authors noted from their review of a number of fraudsters (e.g., potato chips), fraud can be addictive.

Rotten apple theory. Biegelman and Bartow (2012) based this theory on the axiom that it takes one rotten apple to spoil the bunch. In the case of fraud, they theorized that poor leaders who lack integrity and strong ethical principles, and who turn to fraud, can negatively influence their subordinates. Likewise, managers who do not provide proper supervision is also referred to as a bad apple. This theory is also called the culture of noncompliance because there is a failure to follow rules and be accountable when there is no compliance.

Low-hanging fruit theory. Supervisors must not focus only on high-risk fraud such as financial statement fraud. They must also search for low-risk fraud, such as procurement fraud, because there is a high incidence of this type of fraud. In fact, most fraudsters are ultimately caught because a low-hanging fraud has been detected (Biegelman & Bartow, 2012).

Addition by subtraction theory. This concept refers to the fact that it is advantageous for an organization to proactively investigate and detect fraud. Businesses must maintain a zero tolerance for fraudulent activities (Biegelman & Bartow, 2012).

Fraudster as employee theory. This philosophy refers to the notion that after a person has committed fraud against an organization, then he/she should no longer be considered an employee. True employees work hard to ensure the integrity and future of the business. Therefore, these individuals are masquerading as employees to find weaknesses and exploit those flaws to commit fraud (Biegelman & Bartow, 2012).

Although these are not mainstream fraud theories, they aid in better understanding the concepts of fraud. Researchers and forensic accountants have made many observations over time that have resulted in changes to the fraud triangle. These improvements provide insight of why seemingly good people make bad decisions and commit fraudulent acts are represented by the fraud diamond, the fraud pentagon, and the fraud scale. Although these models aid in the study of fraud, Cressey's fraud triangle remains the foundational framework used for fraud analysis and to develop and oversee internal controls.

Characteristics of Fraudsters

Researchers have studied the perpetrators of fraud to determine if there are any similarities that could aid in fraud prevention and detection. Galletta (2015) indicated that most fraudsters are first-time offenders. Also, several authors, Glodstein (2009), Hrncir and Metts (2012), Loria (2015), and Van Gent et al. (2013), pointed out that perpetrators are usually longtime, trusted friends. Hrncir and Metts (2012) emphasized that many employers base their employees' honesty on who they are, such as a family member or a long-time friend or even on the years of service with the organization. Although trust is an important part of any

relationship, employees can take advantage of this notion if adequate internal controls are not in place.

In the Kroll Advisory Solutions (2014) Global Fraud Report, which surveyed 901 senior executives that represented various industries, 74% of the frauds were committed by senior managers or junior employees who were trusted by the owners or board of directors of the organizations. In the *Report to the Nations on Occupational Fraud and Abuse*, which surveyed 114 nations, the Association of Certified Fraud Examiners (2016) conveyed that the United States had the highest percentage of female fraudsters (44.3%). The report also indicated only 8% of fraudsters were fired previously for fraud-related activities. In fact, Trompeter, Carpenter, Jones, and Riley (2014) focused their research on how an individual's past can affect future white-collar criminal acts. Trompeter et al. (2014) considered four interconnected aspects of a fraudster's life: when the crime began, how long the crime lasted, periods of time that the offense ceased, and the patterns in the types of crimes committed. The authors posited that many fraudsters briefly committed relatively minor crimes during adolescence, followed by a period of conformity during their 20s and 30s, and then committed white-collar criminal acts later in life. An important finding was the correlation between the fraudster's level of authority and the length of fraudulent activities. ACFE (2016) found the higher the level of organizational authority, the longer it would take for the fraud to be detected. In fact, ACFE (2016) reported the median duration of owner/executive fraud typically lasted two years as compared to one year for lower-level employees. In addition, Verschoor (2014) indicated there is a direct correlation between the level of the employee and the amount of the fraud loss. He specified although only 18.9% of the fraud was committed by owners and executives, the median loss was $703,000, whereas the ACFE (2016) reported lower-level employees committed 40.9% of the crimes but only caused a

median loss of $65,000. Marais and Ostwalt (2016) reported that in the 2015 KPMG global survey that 79% of the fraudsters were men. Marais and Ostwalt (2016) also found 68% of the perpetrators were between the ages of 36 and 55, 15% were in the 18 to 35 age group, and 8% were older than 55. The authors also explained that 38% of the fraudsters had been with the organization for more than six years; 14%, 4 to 6 years; 19%, 1 to 4 years; and only 2% for less than one year. As far as the level of seniority is concerned, the KPMG report indicated 32% of the fraudsters were considered nonexecutive managers; 26%, executives; 20%, staff members, and 10%, corporate officers, shareholders, and owners. An understanding of the profile of fraudsters helps owners and managers realize that perpetrators can be anyone, including trusted friends and co-workers.

Fraudsters have been grouped into personality risk profiles. Caufield and Steckler (2014) have identified those profiles as situational and deviant fraudsters. Caufield and Steckler described the situational fraudster as an employee who did not join the entity with plans to commit fraud, but believes that he/she has been unjustly treated. Situational fraudsters, according to the authors, typically have a poor work ethic and rationalize fraud as perceived entitlement. Fraud is committed because of weak internal controls which creates an opportunity for the perpetrator. After detection, other employees are typically not surprised because of the poor work ethic of the fraudster. Deviant fraudsters are the most serious threat to organizations. They usually are proactive in their search to commit fraud. Other employees are shocked when they are caught because they are usually trusted, hard-working employees (Caufield & Steckler, 2014). These perpetrators can cause considerable financial loss and public embarrassment to an organization.

Oftentimes, researchers study only the characteristics of individual perpetrators. However, little attention has been paid to co-offending or several fraudsters cooperating to perpetrate a fraud. Free and Murphy (2015) expressed the need for additional research, particularly to determine the reasons for taking the extra risks involved in co-offending. The key to this type of research is to examine the social nature of the crime. Studies show only a partial depiction if researchers only examine the fraudsters individually (Free & Murphy, 2015). They suggest that this type of research emphasizes the "rotten apple rather than the barrel" (p. 19). Since there have been numerous fraud cases that involve more than one fraudster, it would be beneficial to study the rationalization and communal nature of co-offending.

Fraud Prevention

Benjamin Franklin's (1735) axiom that "An ounce of prevention is worth a pound of cure" can be appropriately applied to employee fraud. Businesses must be proactive. Kramer (2015) summarized it best: "Blind trust is not an internal control" (p. 12). Dull (2014), Gannaway (2013), Kollar and Williams (2012), and Singh et al. (2013) identified several fraud prevention techniques, which included safeguarding checks and cash until they are deposited on a daily basis, securing physical access, encouraging employees to report suspected fraud without negative consequences, initiating unscheduled accounting reviews, establishing a code of conduct, and testing employees for drugs. They also recommended that organizations look for repetitive amounts that fall slightly under an amount that requires additional authorization or appear unreasonable. In addition, Levy (2016) and Mangala and Kumari (2015) reported that psychologists indicated that unhappy employees were much more likely to commit fraud. Therefore, Levy (2016) and Mangala and Kumari (2015) rationalized that employee loyalty was a key factor in fraud prevention. They suggested the best method of establishing employee

loyalty is to treat employees fairly. It is much more effective for business organizations to participate in fraud prevention activities rather than have to utilize fraud detection methods.

Opportunities to commit fraud are available in all organizations. While managers cannot control the incentives of fraudsters, they can reduce the opportunities for fraud to occur. In an effort to recommend fraud prevention techniques, Campbell, Butler, and Raiborn (2014) developed the ABC's for reducing fraud potential, which included the following stages: A, which represents ascertain; B, backtrack; C, communicate; D, define; and E, execute. Campbell et al. explained that during the ascertain phase, owners and managers must be aware of the types of fraud opportunities possible within their organizations. The authors pointed out that knowledge of fraud potential does not prevent the crime. Therefore, Campbell et al. recommend that managers should backtrack, review policies and existing internal controls to determine if these procedures are still effective. Communicate refers to creating an anti-fraud climate or tone at the top by developing and implementing a code of ethics for all employees. The define phrase referred to a detailed analysis of fraud prevention and detection techniques as well as developing detailed, specific internal controls related to personnel, vendor, and customer reviews; physical safety measures; purchase amount caps; and conflict-of interest policies (Campbell et al., 2014). Campbell and associates further emphasized the importance of the execute stage, which refers to implementing the internal controls that have been recommended. By recognizing the ABC's of fraud prevention, organizations can become aware of fraud opportunities and mitigate the possibility for fraud.

Employee Red Flags

Fraud risk indicators or red flags were described by Gullkvist and Jokipii (2013) as "events, conditions, situational pressures, opportunities, or personal characteristics that may

cause management employees to commit fraud on behalf of the company or for personal gain" (p. 45). Although the presence of red flags does not guarantee that fraud has occurred, it is an indication that internal controls should be investigated to determine if there are any weaknesses and if those vulnerabilities are being exploited.

Researchers have composed a list of behavioral red flags. Scholars, including Sandhu (2016), Simha and Satyanarayan (2016), and Tschakert et al. (2016), identified the following situations as fraud risk indicators: extravagant lifestyle; financial difficulties; unusually close association with vendor; control issues, such as not taking vacations and being unwilling to share duties; family problems; irritability and defensiveness; addiction problems; domineering personalities; and excessive complaining about inadequate compensation. ACFE (2016) also noted the global statistics for behavioral red flags. They reported only 7% of fraudsters exhibited the behavioral red flag of rejecting vacation time for fear of being detected while 9% of the perpetrators complained about inadequate pay. However, ACFE (2016) noted that living beyond one's means was the most common behavioral red flag, which occurred in 46% of the cases. These fraud risk indicators illustrate there are numerous factors that businesses can look for in an effort to become better aware of potential fraud.

Fraud risk indicators also include signs other than behavioral activities. Verick (2013) created a list of red flags in which business owners and managers should be aware. They listed some concerns, such as repetitive inaccuracies or omissions in financial records; frequent changes in bank accounts; frequent reallocation of funds between accounts; recurrent reclassification of expenses; negative cash flows during periods of earnings growth; frequent payments to one entity; and constant replenishment of petty cash funds. A diligent owner or manager needs to be cognizant of both behavioral and organizational red flags. As a result of

this literature review, the reader of this study will have a better understanding of the internal controls and their impact on employee fraud in small businesses.

Section 2: The Project

The researcher explored the internal controls being used by small businesses in an effort to reduce employee fraud risk in Central Louisiana. The purpose of this multi-case, qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. The researcher collected data through participant interviews, direct- and participant-observation, and documentation analysis. These methods, along with the study of multiple case studies, ensured triangulation as the investigator sought to determine the answer: "How do small businesses in Central Louisiana apply internal controls to mitigate employee fraud risk?"

Section 2 contains a discussion of the purpose of this study along with the role of the researcher and a description of the participants. In a qualitative study, the researcher identifies the research question, designs the study, interviews the participants, transcribes and verifies the interviews, analyzes the data, and reports the findings. The participants were small business owners and/or managers who were members of the Central Louisiana Regional Chamber of Commerce located in Central Louisiana. This section includes a discussion of the research method and design, population, and sampling methodologies used in the study as well as an explanation of the reasons that a qualitative study utilizing case study methodology best answers the research question. In addition, Section 2 covers data collection and data analysis techniques. This section concludes with a discussion of the study's reliability and validity. A study must be both reliable and valid to be replicated and used effectively.

Purpose Statement

The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. Effective internal controls are the first step of defense against employee fraud. Dimitrijevic et al. (2015) posited the risk of employee fraud could be minimized through the implementation of effective internal controls. Further, Tschakert et al. (2016) emphasized the importance of owners and/or managers being able to recognize red flags, which frequently result from ineffective internal controls. Consequently, weak internal controls and owners and/or managers' lack of knowledge of red flags lead to an increased risk from employee fraud. Simha and Satyanarayan (2016) concluded that small business organizations are less likely to invest in the resources of time and money to set-up internal controls than their larger counterparts. They emphasized that investing in fraud prevention education and techniques is essential to decreasing employee fraud risk.

Role of the Researcher

This study was conducted using the case study design under the qualitative methodology in order to gain greater understanding of current practices of the internal control practices used by small businesses and to explore the effectiveness of those controls in preventing employee fraud. The researcher collected data through on site participant interviews, direct- and participant-observations, and documentation analysis. These methods ensured triangulation as the researcher sought to determine answers to *how* and *why* questions.

To properly conduct qualitative research, the investigator must adopt the concept that Geertz (1973) referred to as "researcher as instrument." He explained the investigator and the

research are interwoven so the examiner should contemplate what he/she individually bring to the research and his/her role throughout the process. Also, Yin (2014) argued the ability for researchers to incorporate their experience into a study unites business studies to social sciences such as anthropology, history, psychology, political science, and sociology as well as the fields of education and nursing. Further, Yin explained the importance of having a well-trained researcher to conduct a high-quality research case study because of the continuous interaction between the data being collected and the issues being studied. Yin also expounded on the fact researchers often are required to make judgment calls concerning both technical aspects of a study as well as ethical dilemmas. Kaczynski et al. (2014) shared that research must extend beyond simple data collection to include the exploration of a greater understanding of relationships. It is because of the researchers' comprehensive mindset that investigators gain a more thorough understanding of the phenomena being studied.

The researcher contacted the Central Louisiana Regional Chamber of Commerce located in Alexandria, Louisiana, to obtain a list of small businesses which had fewer than 100 employees. The researcher scheduled an interview with those participants who expressed an interest in the study. During the interviews, the researcher carefully worded the interview questions to engage and communicate with the participants, avoided asking leading questions, and sought comprehensive interviewee responses. Yin (2014) pointed out that case study research does not follow a formal protocol as in other methodologies. Yin clarified that research is about questions and not necessarily about answers because researchers must be able to review the data quickly and continually ask themselves why events or perceptions appear as they do. Through the use of good questions, the researchers' judgments may lead to the need to search for additional evidence. After the interviews, the researcher transcribed the respondents' answers

for analysis and reviewed the participant documentation. To minimize bias in the study, the researcher, as per Yin's (2014) recommendation, was open to contrary evidence and did not use the case study to substantiate a preconceived standpoint. In addition, the researcher was objective in the study since he did not stand to profit from the results of the study or have a previous relationship with the owners and/or managers who participated in the study.

Participants

Although the participants in this case study were not anonymous, the researcher carefully selected the participant based on the study's identifiers. The Central Louisiana Regional Chamber of Commerce provided a list of potential participants in this study. The participants consisted of owners and/or managers of small businesses that had fewer than 100 employees. After obtaining the small business owners' and/or managers' names, email addresses, and telephone numbers, the researcher contacted prospective participants to elicit participation in the study and explained the purpose as well as logistics of the study. According to Yin (2014), the study of a "contemporary phenomenon in its real-world context obligates [the researcher] to important ethical practices akin to those followed in medical research" (p. 78). Therefore, the researcher took care to gain informed consent from all persons who participated in the study and protected their privacy. In the University of Virginia's *Protecting Confidentiality* guide (2017), the authors explained the issue of privacy concerns the participants, whereas confidentiality deals with data. In order to maintain the participants' privacy, the researcher emailed potential participants a consent form to complete for participation in the study, recording the interview, and reviewing the small businesses' documentation, including human resource and financial policy manuals. To maintain confidentiality, the owners and/or managers of five small businesses were studied and designated as participants in the final written report.

Research Method and Design

The effort was best suited to the qualitative research method because personal interviews of key personnel provided exceptional insight into the internal controls used in small businesses and their impact on preventing employee fraud. Effective internal controls are the first step of defense against employee fraud. However, research conducted by the Association of Certified Fraud Examiners (2016) indicated the internal controls employed by small businesses are ineffective and lead to higher levels of employee fraud risk. The researcher sought to gain greater understanding of the current practices of the internal control systems of small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. In this section, the researcher explained his reasoning for conducting a qualitative study and the methodology and design used in this research.

Method

The qualitative method is appropriate to study situations, events, programs, and activities in their natural settings. This method is most appropriate for this study because it utilizes observation and interpretation. Creswell (2014) explained that qualitative research involves combining questions and procedures, data usually collected in the participant's natural setting, data analysis which builds inductively from particulars to general themes, and the researcher's interpretations of the meaning of the data. In addition, he emphasized how the researcher, using multiple sources of data, serves as the key instrument in the study. Sorour and Howell (2013) asserted that qualitative research goes beyond snapshots of *what* or *how many* to actually determining *how* and *why* things happen. Researchers are able to be creative and flexible since the qualitative method focuses on several aspects of a study simultaneously.

In addition to the qualitative approach, researchers may choose to use the quantitative or mixed research methods in their studies. The quantitative method centers on research objectives that involve numerical measurement and analysis in which the objective is to quantify data and measure the occurrences of certain positions. Zikmund et al. (2012) pointed out that one challenge of using quantitative research is that it involves a significant amount of time to develop instruments that contain numerical values which are used in statistical calculations and testing hypotheses. The quantitative method is more objective than the qualitative method since it relies on statistics whereas qualitative does not. Quantitative research is irrefutable and used to recommend a course of action (Park & Park, 2016). Further, Buckley (2015) indicated the quantitative method answers the question of *what* rather than *why* or *how*, as used in the qualitative research approach. Since the purpose of this study is to determine *how* small businesses apply internal controls to mitigate employee fraud risk, the quantitative method is not appropriate for use in this study.

Mixed methods research (MMR) approach combines elements from both qualitative and quantitative research. Creswell et al. (2006) contended the main principle of MMR is that both approaches used together provide a better understanding of the research problem than either single approach. In addition, Venkatesh et al. (2013) reported that typically, quantitative methods are used to test hypotheses, whereas qualitative methods are used to explore a topic. Mixed method research allows the strengths of each approach to compensate for the weaknesses of both qualitative and quantitative research. However, this study is not intended to answer the interrogative question of *what*, but rather to determine *how* the current practices of the internal control systems of small businesses compare with anti-fraud activities recommended by forensic

accountants. Therefore, a qualitative study is needed for this study rather than quantitative or mixed method research.

Research Design

The purpose of a research design was to ensure the data collected enabled the researcher to effectively address the study's problem and answer the research question(s). Singh (2014) identified five designs that researchers may use to frame their qualitative inquiry: case study, ethnography, phenomenology, grounded theory, and narrative.

Researchers use the case study design in qualitative research to gain an in-depth understanding of an individual, family, or organization. Singh (2014) noted this is the preferred method when the researcher is seeking to determine the answers to *how* and *why* questions rather than manipulate variables in a study. Stake (2005) emphasized that case studies gain reliability by diligently triangulating the reports and interpretations continuously throughout study. Creswell (2013) and Stake (2005) explained the case study design uses various sources of information, such as documentation, interviews, and direct- and participant-observation as means to gather data. Moreover, Starman (2013) and Yin (2014) acknowledged that case studies have been used in social sciences and are valued in practice-oriented fields, such as education, public administration, and management. Guercini (2014) also declared the case study method has increased in popularity, especially in industrial marketing, management, and entrepreneurship research.

Other types of qualitative design include ethnography, phenomenology, grounded theory, and narrative. Ethnographic research is probably the most familiar design of qualitative research. According to Cordoba-Pachon and Loureiro-Koechlin (2015) and Grossoehme (2014), in this type of study, which began in the field of anthropology, a researcher engages himself in

the participant's environment to understand the culture, goals, and challenges in that situation. They explained this type of research is not based on simple interviews, but observations that may require years for the researcher to become fully immerged in the setting. Creswell (2013) pointed out that in an ethnography, the researcher explains and interprets the learned patterns of behaviors, beliefs, language, and values of an entire culture-sharing group, people who interact over time.

A phenomenological study is the appropriate qualitative method to use when the researcher wants to describe an activity, event, or a phenomenon based on the participant's experience. Mosalanejad et al. (2014) explained that through interviews, watching videos, reading documentation, visiting locations, or participating in events, the researcher can gain an understanding of the participant's perception of an event. In addition, Snelgrove (2014) highlighted the subjective nature of phenomenology. Snelgrove emphasized that phenomenological research is the best method to use when one wants to study what an experience or event means to a particular person or group of people.

While a phenomenological study is used to describe an event, the grounded theory approach, postulated by Glaser and Strauss in 1967, provides a theory or explanation of *why* an event occurs. Glaser (2014) emphasized that grounded theory enables the researcher to see a situation as it actually exists without prejudice. Likewise, Webster (2016) clarified this technique is inductive in nature in that it permits the researcher to examine the means that their subjects utilize to solve their concerns. A benefit of using grounded theory is it adopts a neutral view of human actions by avoiding researcher assumptions. Creswell (2013) explained that grounded theory is the best approach to use when a theory is not available to understand or explain the steps in a process.

In the narrative method, researchers limit the participants to one or two people in order to develop a persona. Jeppesen (2016) clarified that with the narrative design, researchers use ordinary literary methods to create a story that interweaves a sequence of events. Narrative research is typically used in the sciences, particularly in describing the participants' health issues.

Since the case study design is used to conduct an in-depth study of contemporary phenomena and answers the questions of *how* and *why*, the researcher determined it was the best method to use. In this study, the researcher explored the internal controls systems of small businesses located in Central Louisiana by using participant interviews with small business owners and/or managers, direct- and participant-observation, and documentation analysis. Since the sample was from one location, Central Louisiana, and the focus was specific in nature, internal controls, the case study research design was the best and most fitting design for this study. The researcher conducted multiple case studies and ultimately draw cross-set conclusions.

Population and Sampling

The population for this study was drawn from the 1,004 small businesses that are members of the Central Louisiana Regional Chamber of Commerce and that employ fewer than 100 personnel. Latham (2014) pointed out that in a qualitative research study, the number of participants is determined when saturation has occurred. In other words, when additional participants do not provide additional information, insights, or themes, there is no need for subsequent interviews. Creswell (2013) strongly advised that researchers not include more than 4 or 5 case studies in a single study. He explained this number should provide sufficient opportunity to identify themes of the cases as well as conduct cross-case analysis. Additionally,

Crouch and McKenzie (2006) advised that fewer participants allow the researcher to establish and maintain good rapport with the participants.

Creswell (2013) recommended that participants for qualitative research be intentionally selected from the population. Therefore, the researcher followed the selection process provided by Creswell (2014) to determine the participants for this study. First, the researcher obtained a list of 1,004 small businesses from the Central Louisiana Regional Chamber of Commerce. The researcher used the random sampling technique to select five small business organizations from the population. The participants in this study consisted of the owner and/or manager of each small business. They had the knowledge, awareness, and experience of internal controls.

Data Collection

To collect data for this study, the researcher contacted five small businesses from a membership list provided by the Central Louisiana Regional Chamber of Commerce. The researcher conducted face-to-face interviews with the owners and/or managers of each organization over a three-week period of time. Each participant responded to a 44-question survey. The researcher then transcribed the interviews, and respondents verified the accuracy of the transcripts. In addition, the researcher reviewed relevant documents, such as employee manuals and written procedures. The researcher organized the data, first, by transcribing the interviews. Next, an annotated bibliography was created, which made note of important information for each document. Then, the researcher created a table which indicated a description of the source of data along with the number of notes. Finally, the researcher generated narratives for each case study to assist in the data analysis phase. The data collection, which consisted of the instruments, data collection techniques, and data organization, will be discussed.

Instruments

The researcher serves as the primary instrument for a qualitative study. Pezalla, Pettigrew, and Miller-Day (2012) explained that "researcher-as-instrument" refers to the concept that the researcher is an active participant in the research process. Pezalla et al. elaborated that it is through the researcher's interaction that respondents feel safe to share experiences. Additionally, Poggenpoel and Myburgh (2003) pointed out it is the researcher who directs the flow of information, identifies participant cues, sets the respondents at ease, and translates and interprets participant data into meaningful information. In qualitative research, the researcher brings his/her tacit knowledge, subjectivity, and perspective to the study (Essays, UK, 2015). Further, Barrett (2007) expounded on the researcher's impact on the data collected, organized, and transcribed. Since the researcher analyzes the data, establishes codes to determine patterns in the data, and ascertains themes that develop, data analysis and interpretation are frequently interwoven and rely upon the researcher's knowledge of the field under study, reasoning, and creativity.

The researcher developed open-ended questions based on the five components of the model for assessing internal business controls, proposed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The five components of the model include factors in the following areas: control environment; risk assessment; control activities, such as human resources, cash receipts and disbursements, and purchasing and inventory; information and communication; and monitoring (Cotton et al., 2016). Doody and Noonan (2013) recommended the use of open-ended questions for qualitative research so that the participants can respond in their own words. Also, the authors explained that interviews are the most frequently used method of data collection. They cited the preference for using interviews

because the participants perceive the interview process as “just talking.” In an effort to increase the reliability of the instrument, the researcher used the same criteria and wording for all participants. After the interviews were transcribed, the researcher used respondent validation by allowing the participants to verify the accuracy of the transcripts.

After making an appointment with the participant, the researcher met in the business owner and/or manager’s preferred location to conduct the interview. He used predetermined questions for each interview, but asked clarifying, probing questions and/or discussed new topics that emerged from the interviews. The researcher was able to organize the interview questions through the use of an interview guide that contained 44 open-ended questions. The interviews ran about one hour and were recorded and then transcribed for further analysis. By using open-ended questions with a semi-structured format, the small business owners and/or managers were able to discuss their organizations’ internal controls in a logical order and the researcher was able to ensure the five components of the COSO model for assessing internal business controls were examined.

Stake (2005) emphasized that case studies gain reliability by triangulating the reports and interpretations continuously throughout the study. Moreover, Yeasim and Rahman (2012) described four types of triangulation used in qualitative research: data triangulation, in which data is gathered from two or more different sources; investigator triangulation, which utilizes multiple observers to gather and interpret data; theoretical triangulation, in which the researcher uses more than one theoretical position when interpreting data; and methodological triangulation, where more than one research method or data collection technique is used. In this study, the researcher used data triangulation.

Yin (2014) asserted that interviews are one of the most important sources of data collection for case studies. He expounded on the importance of using an interview guide to minimize researcher bias. In addition, the author explained the importance of asking relevant questions. In this study, the researcher developed carefully constructed interview questions that were adapted from Williams and Kollar's (2013) *Journal of Accountancy* article entitled "What are the Risks?" They pointed out that small businesses, companies with fewer than 100 employees, are often challenged by preventing and detecting employee fraud. Their survey was designed to aid owners and/or managers determine if internal controls appear to be in place that will aid in the prevention of fraud or if the processes need to be reviewed and modified to improve controls. In this article, the authors presented a self-assessment tool that they had created to evaluate the internal controls of small businesses. They used three professional publications to develop this assessment instrument: *Audit Risk Assessment Tool and Guide*, published by the Association for the Institute of Certified Public Accountants' (AICPA; n.d.); *Managing the Business Risk of Fraud: A Practical Guide,* written by the Association for the Institute of Certified Public Accountants (n.d.); and *Common Fraud: A Guide to Thwarting the Top Ten*, written by Helms (2012). Yin (2014) also suggested several ways that researchers can use to eliminate bias. For example, in this study, the researcher reflected on his own ability to be unbiased as well as sought respondent validation where participants confirmed and provided feedback for the interview transcripts.

Data Collection Techniques

Yin (2014) explained that three principles are involved with data collection: maintaining a chain of evidence, creating a case study database, and using multiple sources. Additionally, Yin explained there are six sources that can be used to establish a chain of evidence:

documentation, archival records, interviews, direct observation, participant-observation, and physical artifacts. Further, the Yin (2014) discussed the importance of using a database which organizes the data and analysis in one location or document, including notes, narratives, tabular material, and documents. Creswell (2013), Stake (2005), and Yates and Leggett (2016) noted the case study design utilizes multiple sources of information, such as documentation, interviews, and direct- and participant-observation, as means to gather data.

Doody and Noonan (2013) described some of the advantages of using interviews for data collection. First, Doody and Noonan explained that interviews help the researcher to establish rapport with the participants as well as allowing the researcher to be able to make observations while listening to the responses. Then, Doody and Noonan (2013) highlighted the interviews allowed researchers to probe participants' responses and permitted more complex questions. After the interview dialog was transcribed, respondents participated in member checking, or participant verification, by reviewing the accuracy of the transcripts (Birt, Scott, & Cavers, 2016). In addition to the interviews, the researcher also reviewed relevant documents, which included recruitment and hiring procedures, employee manuals, written practices for cash receipts and disbursements, and procedures for purchasing and inventory.

Data Organization Techniques

Yin (2014) recommended that data be organized for case studies as a database with four sections: case study notes, documents, tabular materials, and narratives. After detailed interviews with the owners and/or managers of five small businesses and a review of numerous documents, the data were organized according to Yin's recommendation. First, participant interviews were transcribed. Second, the researcher created an annotated bibliography which summarized key information for each document, including page and paragraph numbers. Third,

the researcher created a table which showed the number of notes and a description of the source. Although this tabular file was not used for analysis, this technique aided in the ability to easily locate data needed for analysis. Fourth, the researcher created narratives for each case study which assisted in the data analysis phase. The researcher used Microsoft® Office Word for transcribing interviews and making field notes and Microsoft® Office Excel to create a log of the different types of documents and records.

Confidentiality and security are also concerns for data organization. The data for this study were saved on a password-protected laptop as well as backed up on a password-protected external hard drive. Also, hard copies of documents and original handwritten notes were secured in a locked file cabinet. The researcher and dissertation chair were the only people who had access to these digital and hard-copy files.

Data Analysis Techniques

The researcher must analyze data in a qualitative research study to make it understandable and useable. Creswell (2014) described two approaches that can be used in data analysis: inductive and deductive. In the inductive approach, the researcher organizes the data into five to seven themes. In the deductive approach, the researcher determines if additional information should be gathered to support each theme. In this study, the researcher began with the inductive approach and ended with the deductive approach.

Data analysis for case studies can be challenging because of the sheer volume of qualitative data collected. Yin (2014) pointed out that analysis often occurs concurrently as data is collected. He described the following five analytic techniques:

(1) pattern matching is comparing patterns predicted prior to data collection with those patterns determined from the collected data;

(2) explanation building is a special type of pattern matching which determines the cause of how or why something happened;

(3) time-series analysis compares a theoretically important trend identified before the case study to the study's observed (empirical) trend;

(4) logic models is a special type of pattern matching which involves the staging of events in a repeated cause-effect-cause-effect sequence and then compares observed events to theoretically anticipated events; and

(5) cross-case synthesis involves analyzing multiple cases and aggregating the findings across the cases by utilizing one of the other four techniques.

In this study, the researcher used the data analysis techniques of explanation building to explain how small business owners and/or managers implemented internal controls and cross-case synthesis to combine the findings of the five separate cases.

There are five steps in the process of conducting qualitative data analysis. According to Creswell (2013), these steps include: (a) organizing and preparing the data, (b) reading all data and memoing, (c) coding and organizing the data into themes, (d) interpreting the data, and (e) representing the data. In this study, first, the researcher organized and prepared the data by transcribing the interviews, typing the field notes, cataloging all of the documents, and sorting the records into the different types. The researcher provided the participants of the study with a copy of his/her transcript so its accuracy could be verified. Harper and Cole (2012) explained that member checking is a quality control process that is used in qualitative research to improve the accuracy, validity, and credibility of the respondents' interviews. Second, the investigator carefully read all of the data, noting potential themes in the data collected. By analyzing various documents from the small businesses, the researcher gained additional insight into the

communication techniques and information provided to their employees. The researcher made memos on the interview transcripts. Third, the researcher coded the data by organizing it into categories and assigning a descriptive word to each segment. Fourth, the researcher formulated natural generalizations of what was learned in the study. The investigator interpreted the findings to determine internal control weaknesses and developed a plan to minimize the risk of fraud in the organizations. Fifth, the researcher used qualitative narrative to present a detailed illustration of the findings. These steps were completed for each of the five cases. After completion of each individual analysis, the researcher conducted a cross-case analysis.

Reliability and Validity

Roberts, Priest, and Traynor (2006) explained that reliability and validity are ways of demonstrating and communicating the trustworthiness of the study's findings and the thoroughness of research processes. Leung (2015) described reliability as the ability to replicate the research process and the results, whereas he defined validity as the appropriateness of the processes, tools, and data. Although there are no unanimously established criteria for assessing reliability and validity in qualitative research, there are some common strategies that can be implemented to reduce threats to the trustworthiness and accuracy of the study. Some of the strategies include eliminating researcher bias, participant validation of data collection, meticulous record keeping which demonstrates a step-by-step data collection and analysis process, and data triangulation (Creswell, 2013; Noble & Smith, 2015). For research to be beneficial, it should avoid misleading those who use it.

Reliability

In qualitative research, the reliability of a study is determined by its consistency or trustworthiness. Morse (2015) explained the strategies for determining trustworthiness in

qualitative research were postulated by Guba and Lincoln in the 1980s when they used the terms dependability, credibility, and transferability instead of rigor, reliability, and validity. Likewise, DeVault (2017) described the necessary components for a study to be trustworthy: credibility, transferability, dependability, and confirmability. DeVault (2017) explained that credibility can be established through triangulation and member checks. Further, Shenton (2004) expounded on the concepts of transferability, dependability, and confirmability. Shenton (2004) clarified that transferability is achieved when the researcher provides enough detail of the study for the reader to be able to decide if the findings can be applied to other settings. Although it is difficult to achieve in qualitative research, Shenton noted that researchers should strive for dependability in which future investigators can repeat the study. Confirmability can be achieved by demonstrating the findings were developed from the data rather than from the researcher's presuppositions (Shenton, 2004).

Creswell (2014) suggested the researcher should be concerned with the reliability of the research prior to the study itself. Creswell recommended the researcher should have no previous relationships with participants to minimize biases. In addition, Yin (2014) emphasized the importance of accurately recording and transcribing interviews. Further, Roberts et al. (2006) pointed out the importance of noting non-verbal communication. In addition, Creswell (2013) suggested the use of open-ended questions with the same criteria and wording for all participants. Creswell also emphasized the importance of allowing participants and possibly colleagues to review interview transcripts to verify the accuracy. Likewise, Noble and Smith (2015) recommended using low interference descriptors, verbatim examples of participants' comments, in written accounts of the finding.

For this study, the researcher selected small businesses in which there was no previous relationship with the researcher. Also, the researcher kept and securely stored emails, consent forms, and recordings of the responses to the questions during data collection. The investigator maintained detailed records, such as the time of day, setting, and non-verbal communication during and after the interviews. In addition, the researcher used the semi-structured interview approach with identical wording and open-ended questions to ensure the consistency of the responses. The researcher accurately recorded and transcribed the interviews and compared the written transcripts with the recorded verbal answers to ensure accuracy. The participants then verified the accuracy of the transcripts. In the findings section of the final research report, the researcher included participants' verbatim quotes to add credibility to the findings.

Validity

The validity of a study refers to how accurately the research findings represent the concept that it claims to measure (Roberts et al., 2006; Yates & Leggett, 2016; Yin, 2014). It indicates the thoroughness of the research. Creswell (2013) summarized his view of validity in qualitative research as an effort to evaluate the accuracy of the findings. Creswell added that advantages in seeking validation of a study include the amount of time spent in fieldwork and the comradery established between the researcher and the participants. Although the author prefers to use the term validation rather than the term verification, which is used in quantitative research, qualitative researchers must choose which types and terms with which they are comfortable. Creswell (2013) recommended that researchers use at least two validation strategies in their qualitative research. Creswell focused on eight techniques that researchers could use to ensure validity: prolonged engagement and persistent observation; triangulation; peer reviews; negative case analysis; clarifying researcher bias; member checking; rich, thick descriptions; and external

audits. Similarly, Leung (2015) suggested that validity can be authenticated by one of three possible methods. One method is to use contradictory evidence or deviant cases, which is used to explore any potential researcher bias. The second method is through respondent validation, in which the participants are provided with an opportunity to review the data and the findings for accuracy. The third method employs constant comparison, which is the ability to compare individual data to a larger set of data for steadfastness (Leung, 2015; Yates & Leggett, 2016). Ideally, researchers should use triangulation, which uses at least two of these methods, to enhance validity (Noble & Smith, 2015). In this study, the researcher used multiple case studies to triangulate findings, as suggested by Yates and Leggett (2016).

Researchers must be aware of potential researcher bias. Roberts et al. (2006) explained that bias can be the result of preconceived ideas of the researcher based on familiarity with the participants or with the setting of the study. Likewise, Noble and Smith (2015) reiterated that this is particularly challenging with interview data. In this study, the researcher did not have any previous relationships with the participants. Roberts et al. (2006) advocated a process called reflexivity, in which the researcher openly reflects on his own ability to be unbiased. The researcher included this reflection in the final written study. Further, bias was also minimized by respondent validation where participants confirmed, revised, and provided feedback. Reliability and validity are two concerns which a qualitative researcher should consider while designing a study, analyzing outcomes, and evaluating the quality of the study.

Transition and Summary

In Section 2, the researcher described the research method and design, the role of the researcher, and the participants. Furthermore, the investigator presented the data collection,

organization, and analysis techniques. Finally, the researcher explained the concepts of reliability and validly.

The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. To this end, the researcher explored the internal controls systems of small businesses located in Central Louisiana that employed fewer than 100 employees and were members of the Central Louisiana Regional Chamber of Commerce located in Alexandria, Louisiana. The researcher used participant interviews with small business owners and/or managers, direct- and participant-observation, and documentation analysis. The researcher developed open-ended questions based on the five components of the model for assessing internal business controls, proposed by COSO: control environment; risk assessment; control activities; information and communication; and monitoring. The researcher also reviewed associated documents, such as recruitment and hiring procedures, employee manuals, written practices for cash receipts and disbursements, and procedures for purchasing and inventory.

The researcher organized the data to make analysis less complicated and transcribed participant interviews. Since security and confidentiality were concerns, the researcher saved the data on a password-protected laptop as well as backed up on a password-protected external hard drive. Also, hard copies of documents and original handwritten notes were secured in a locked file cabinet. The researcher used several strategies to ensure the reliability and validity of the study. For this study, the researcher selected small businesses in which there was no previous relationship with the researcher to eliminate bias. The researcher carefully recorded and transcribed the interviews and compared the written transcripts with the recorded verbal answers

to ensure accuracy. The participants then verified the accuracy of the transcripts. Multiple case studies were used to triangulate findings.

Section 3 presents the findings from the research and how the findings will be applied to professional practice. As an active member of the Louisiana Society of CPAs and an accounting professor at a local university, the researcher expects to share the findings of this study with these organizations. In addition, the researcher provides recommendations for action and further study, based on the findings, to enhance the area current practices of the internal control systems of small businesses and improve the effectiveness of their systems.

Section 3: Application to Professional Practice and Implications for Change

Section 3 begins with a brief overview of the study, which includes a review of the study's purpose, research question, and process. Then, the researcher presents the findings of the study and how this study applies to professional practices. Next, the researcher provides recommendations for action for those people affected by the study and identifies recommendations for further study. In addition, the researcher reflects upon his experience with the research process and the relationship between biblical principles and the study. Finally, the researcher concludes with a summary of the pertinent aspects of the study and how this research has closed a gap in the literature.

Overview of the Study

The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and to explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants. Weak internal controls can lead to increased fraud risk. The conceptual framework of this study consisted of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management (ERM), International Organization for Standardization (ISO), fraud triangle, and routine activities theories (RAT). These models were used to frame the study and develop the five themes, which are control environment, risk assessment, control activities, information and communication, and monitoring. Since the objective of the interviews in this multi-case study was to gain greater understanding of the current practices of the internal control systems, the central research question was: "How do small businesses in central Louisiana apply internal controls to mitigate employee fraud risk?"

The researcher carefully selected the participants based on the study's parameters. The Central Louisiana Regional Chamber of Commerce provided a list of potential participants in this study. According to Mittelstaedt, Harben, and Ward (2003), small businesses are defined as those with fewer than 100 employees. Each of the businesses studied met this criteria and were all members of the Central Louisiana Chamber of Commerce. In determining the number of small businesses to study, the researcher used Creswell's (2013) recommendation that no more than four or five case studies be included in a single study. Creswell (2013) explained that this number should provide sufficient opportunity to identify themes of the cases as well as conduct cross-case analysis. In this study, saturation occurred after five small business owners and/or managers had been interviewed. In other words, additional participants would not have provided additional themes or information. Therefore, the researcher did not interview additional participants. The researcher performed data triangulation by recording and transcribing interviews with five small business owners and/or managers in central Louisiana, reviewing and analyzing company documentation, interpreting data, making observations, and offering recommendations.

The initial step in accomplishing the purpose of this study was to develop interview questions that modeled the five components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed in 1992 and revised in 2013. The five components of the model, which were described in the conceptual framework, are control environment, risk assessment, control activities, information and communication, and monitoring. The researcher developed a 44-question interview (see Appendix A). Next, the owner and/or manager from each business participated in a one-on-one, semi-structured interview with the researcher. The researcher then transcribed the interviews and validated the

accuracy of the transcripts with the participants. Then, the researcher made memos on the interview transcripts. Next, the researcher coded the data by organizing it into categories, the five elements of the COSO model. Subsequently, the researcher created a master summary table which identified the findings from each of the interviews from the five participants. Finally, after reviewing documents from the small businesses, such as employee manuals, job descriptions, and written policies and procedures, the researcher provided recommendations for those organizations affected by the study.

Data analysis for case studies can be challenging because of the sheer volume of qualitative data collected. In this study, the researcher utilized two of the data analysis techniques identified by Yin (2014). The researcher applied explanation building to determine how small business owners and/or managers implemented internal controls and cross-case synthesis to combine the findings of the five separate small businesses (Yin, 2014).

The researcher analyzed the data in this research study to make it understandable and useable. Creswell (2014) described two approaches that can be used in data analysis: inductive and deductive. In the inductive approach, the researcher organizes the data into five to seven themes, whereas in the deductive approach, the researcher determines if additional information should be gathered to support each theme. In this study, the researcher began with the inductive approach and ended with the deductive approach.

An analysis of the interview responses indicated that all of the owners of the small businesses demonstrated an active role in all of the functions of their businesses. The small business owners and/or managers evaluated financial, strategic, operational, and compliance risk assessment on a regular basis. In addition, the owners and/or managers of the organizations implemented various control activities that helped achieve organizational objectives by

alleviating risks, such as developing and implementing well-designed employment; payroll; cash management, including receipts and disbursement; and purchasing processes. The information and communication varied among the businesses, ranging from offering a detailed employee manual as well as annual ethics and anti-fraud training to lacking an employee manual and employee training. These small businesses exhibited solid monitoring, which included internal and external audits, ethics and conflict of interest policies and inventory management.

After conducting, reviewing, and transcribing the interview responses, analyzing company documentation, and making observations, the researcher gained a greater understanding of the current practices of the internal control systems of selected small businesses and explored the effectiveness of their systems.

Presentation of the Findings

The presentation of the findings of this qualitative analysis included interpretations related to the literature review and conceptual framework that address the central research question: "How do small businesses in central Louisiana apply internal controls to mitigate employee fraud risk?" The businesses in this study were all privately held corporations from a variety of industries including the hospitality, health services, financial services, heating, ventilation, and air conditioning (HVAC), and office supplies. They ranged in size from 19 to 93 employees, with one to five owners. The diversity of industries represented by these organizations provided the researcher with a broad scope from which to gather data. Moreover, despite the diversity in the industries represented, there were many similarities associated with the findings. Interestingly, the researcher was surprised by the results of this study in comparison to the limited previous research concerning small businesses, such as the ACFE's 2016 *Report to the Nations* and the U.S. Chamber of Commerce Small Business Nation (2009).

Those studies indicated small businesses were particularly vulnerable to employee fraud because they have fewer internal controls. In fact, check tampering, skimming, payroll, and cash larceny schemes all occurred over twice as frequently in small businesses as in their larger counterparts. Additionally, 30% of small business failures were the result of employee fraud. In this study, the researcher found that in some areas there were more internal controls in place. For example, owners and/or managers were significantly more involved in the operations of the small businesses studied and performed more external auditing of the financial statements and internal controls. The findings of the study were presented according to the five components of the COSO model: control environment, risk assessment, control activities, information and communication, and monitoring.

Control Environment

The researcher studied each participant's organization to ascertain how their small business applied internal controls related to the control environment to mitigate fraud risk. The control environment focuses on risk management within the business organization. Consequently, it forms the foundation for the other four components in COSO's model. Since Rae et al. (2017) noted all of the aspects of the control environment included characteristics of integrity, this element of the model may also be considered to be the ethical environment of an organization. Laxman et al. (2014) explained that as part of the control environment, it is necessary to establish an anti-fraud organizational culture, promote owner and/or manager involvement in business activities, and maintain an ethics hotline.

Anti-fraud organizational culture. Henry (2016) emphasized that a control environment exhibits the importance of anti-fraud measures to an organization's employees. The tone at the top of an organization, which includes the organizational structure, has a significant

effect on the probability and frequency of fraud. Tone at the top is defined by Patelli and Pedrini (2015) as an atmosphere created by owners, board of directors, or chief executive officers. Accordingly, Hambrick and Mason (1984) developed the upper echelons theory holding that persons in high positions of authority within an organization have a substantial impact on organizational practices. Also, Murphy and Free (2016) and Wilkins and Haun (2014) described how the tone at the top is influenced by management's integrity, attitude, and ethical values. They explained that when management encourages high ethical standards, the organization is less likely to be vulnerable to fraudulent activities. One participant in this study demonstrated ethical values by actively inquiring about possible fraudulent activities by conducting quarterly one-on-one interviews with every employee. The participant indicated the following question was asked during the quarterly interviews: "Are you aware of any fraudulent activity or anything that you need to report to management?" Also, the managers asked the same question annually in the review process and in an exit interview after termination, either voluntarily or involuntarily. The participant explained:

> Employees are encouraged [to report concerns of fraudulent activities to owners] because we try to make sure that they understand that this is their company, too. If they take ownership and pride in our company . . . and they see someone doing something that is not for the company's good, they will report it.

Another method of establishing an anti-fraud culture is by vetting and selecting ethical vendors. Four of the participants indicated that the owners selected the vendors. One participant described the vetting process for potential vendors—indicating that the general manager selected vendors after having reviewed at least three references from each prospective vendor. The other

participants stated that the owners selected vendors personally. One participant elaborated on the importance of selecting ethical vendors:

> We do not to do business with people who sell products that are not what they say they are. You have to be very careful about that. I'm not going to do business with someone who's not [ethical]. It trickles down. So, if we find a vendor or a customer that's unethical, we just won't do business with them anymore.

Patelli and Pedrini (2015) expounded on the "trickle-down" theory, explaining that the leadership of the top echelon of an organization influences ethical conduct in the lower levels of the workplace. One owner discovered there were "a lot of vendors that you don't want to do business with. We are very much connected with making sure that we are ethically on point."

All of the participants in this study established an ethically strong tone at the top compared to the findings of the Ethics Resource Center (2013) which reported that 60% of misconduct involved someone from the supervisory level up to those individuals holding top management positions. In fact, 24% involved senior managers. The tone at the top creates an environment that encourages either integrity or unethical behavior.

Owner and/or/manager involvement. When owners and/or managers are actively involved in their businesses, fraud risk is usually diminished (Glodstein, 2015; Klein, 2015; Levy, 2016; McCole, 2014; Stone, 2016). Glodstein (2015) also recommended that owners regularly review accounting documents, such as bank statements, cancelled checks, payroll expense reports, and cash receipts and disbursements. One participant stated, "The owners are involved in pretty much everything . . . oversight of compliance and expenses, vendor approval . . . reviewing bank statements and financial records . . . and signing checks over a certain amount." According to Hrncir and Metts (2012) and Verick (2013), if only one or two people

are involved in the accounting process, the owner should be actively involved by knowing the particulars of the organization's revenue and expenses. One participant prepared a daily report to the owner which included account balances, available credit limits, pending withdrawals, and pending deposits. Not only did the preparation of this report compel the general manager to look at this information daily, it also enabled the owner to review the financial position of the organization each day. The participant explained, "The owner is very, very involved in the financial status of this business. The owner's mind is very brilliant and holds the bank balances in his head for all of his accounts." Another participant indicated the owners, CEO, and accounting manager met weekly to review the financial statements, sign checks, prepare a cash flow statement, and approve purchases over a specific dollar amount. In addition, the owners met at least twice annually to review the strategic and operational plans. Another participant explained the daily routine:

> We begin the workday by ensuring that everyone is here . . . that we don't have issues on deliveries . . . that the drivers are all loading their trucks . . . and that the customer service people are at their desks. I get a sense of the atmosphere [of the business].

The owner was also very involved in accounts receivable and accounts payable and explained, "In a business, there are lot of people issues . . . how the people are doing. If you have good people, then you have a good company." There are many aspects with the interworking of a small business, so it is imperative that owners and/or managers be actively involved in the regular activities of the business.

In each of the businesses, the owners were involved with the decision-making processes, though with some variation in their methods. In one business, the general manager prepared a daily financial report for the owner, whereas the owners in the other four businesses met with the

management team weekly to review the finances and concerns of the organizations. Currently, there is limited data concerning owner and/or management involvement in small businesses.

Ethics hotline. Organizations that use hotlines significantly reduce losses due to fraud. The ACFE Report to the Nations (2016) held the use of hotlines was the most common method that fraud was detected. Yet, the report cited only 18% of small businesses implemented hotlines whereas 82% of large organizations provided them. Zhang et al. (2013) explained the goal in providing hotlines is to decrease the tipster's hesitation to become involved in the situation. In this study, none of the businesses provided hotlines for their employees; however, they all had an open-door policy for employees to talk with the owner(s) about their concerns, which was an effective internal control to reduce employee fraud risk. In addition, one of the participants explained the employee manual also contained the procedure for contacting the employee's supervisor. He elaborated:

> One of the [policies] . . . that is used [in the employee manual] is that if you ever feel like you're treated poorly by in-house management . . . or [suspect] fraudulent activity, it is elevated to the next person in line, which is generally the CEO.

One participant indicated the leadership of the firm was proactive in its attempt to discover fraud. There was a compliance plan that described "the whistleblower guidelines and safe harbors that can be used for reporting so that there will be no consequence of reporting suspicions."

The researcher determined there was a healthy control environment in the selected small businesses in central Louisiana which mitigated employee fraud risk. For example, 100% of the organizations encouraged an anti-fraud organizational culture and high ethical standards by

vetting and using ethical vendors. In addition, all of the owners and/or managers were actively involved in business decisions.

Risk Assessment

All organizations face both internal and external risks. Frazier (2016) emphasized the importance of determining organizational objectives prior to risk assessment so that risks can be identified and analyzed in accordance with the business' goals. It is important to evaluate potential fraud and determine appropriate means to respond to significant fraud risk. Power (2013) explained that fraud risk focuses on internal control systems, risk, and managerial responsibility. Wilkins and Haun (2014) indicated that fraud assessment not only concerns minimizing risks but also managing them. The authors acknowledged the four areas that should be evaluated in risk assessment, according to COSO, include financial, strategic, operational, and compliance.

The researcher referred to the Enterprise Risk Management (ERM) Integrated Framework in framing the interview questions in order to address the central research question. McNally (2015) described the 2004 ERM as a complementary model to COSO's internal control framework. The author explained the outline provides direction to businesses in an effort to assist them develop and apply enterprise risk management assessment into three areas: event identification, risk assessment, and risk response. In addition, the researcher referred to the International Organization for Standardization (ISO; 2009), which provides principles and guidelines of risk management in order to help businesses achieve their objectives, identify threats, and allocate resources for risk management. Effective risk management must be systematic, structured, and timely. The COSO and the ISO both offer frameworks that improve the effectiveness of organizational risk management and internal control activities (McNally,

2015). Therefore, the researcher found these guidelines helpful in analyzing each small business' risk assessment.

The researcher asked the participants to describe the risk assessments conducted by their businesses, which varied by industry. For instance, the participants in industries that required government regulations were concerned with compliance assessment whereas another participant focused on weekly assessment of competitors. One participant described the many types of financial, strategic, and operational risk assessments that the business managers conducted. For example, the owner and/or manager monitored insurance and interest rates daily as well as checked the lines of credit. The participant explained:

> As far as workers' comp assessments, they are conducted on a monthly basis. We're considered a self-insured fund through one of the local state associations, so that is something that is processed against our payroll on a bi-weekly basis as well.

Two participants conducted many compliance risk assessments. Both of these organizations had a Compliance and Risk Management Department or a specific employee responsible for ensuring compliance and assessing risk. In fact, the health services business had to be in compliance with HIPAA (Health Insurance Portability and Accountability Act) which protects patients' privacy concerning their medical records. It was also quite active in strategic risk assessment, resulting in its business adding ten sites.

Gilmore-Allen (2015) explained that organizations must perform risk assessment, specifically for potential fraud with regard to technology. The author suggested that organizations need privacy and security policies concerning the use of strong passwords, social media, email, and routine password changes. Gilmore-Allen (2015) emphasized the importance of including safeguards to avoid technology fraud in their employee training. One participant

was concerned with assessing risk through its technology. The participant explained, "We do an annual technology risk assessment audit on our databases…using our external technology group." Two participants explained that they had to be compliant with OSHA (Occupational Safety and Health Administration of the United States Department of Labor) regulations. Another participant emphasized the risk assessment concerning competition. The participant stated, "Every week, we are looking at what's the competition out there, what are they doing, what are they selling, what are you up against, what are your issues." In addition, the participant expressed concern with the safety and liability of its delivery drivers. In fact, the participant indicated the business "installed a program that if our driver goes 10 miles over the speed limit, we get an email."

One participant summarized the importance of risk assessment:

> Overall, in the four properties, risk assessments are conducted probably more regularly than they would in a larger scale company. The reason I think that takes place is because there's a lot more at stake for one person versus a board of directors or a board of investors.

All of the businesses performed both internal and external risk assessments. Because of the nature of their organizations, the participants of three businesses were careful about compliance risk assessment. The researcher found while financial risk was assessed by four of the participants, there was limited financial risk assessment by one of the small businesses. Fundamentally, risk assessment concerns an organization's future, which is managed in the present. The small businesses owners and/or managers interviewed utilized an effective assortment of risk assessments to reduce the risk of employee fraud.

Control Activities

Wilkins and Haun (2014) described control activities as procedures defined through policies so that organizational objectives can be achieved by alleviating risks. Further, Verovska (2014) elaborated that owners and/or managers chose internal controls based upon the organization's structure, type of industry, and management's attitude concerning internal control. Also, Rittenberg (2006) recommended that organizations should consider if a potential internal control minimizes risk to a satisfactory level, is cost effective, and falls into the category of one of the COSO framework's five components of effective internal control. The control activities portion of the interviews included questions concerning background checks during the hiring process, securing the payroll process, establishing job rotation and mandatory vacation policies, applying policies for separation of duties, designing a procedure for handling cash receipts and disbursements, and creating a process for making purchases and safeguarding inventory. Managers should implement and design anti-fraud methods by evaluating current controls and establishing new ones to reduce the risk of employee fraud.

Background checks. Past performance is a good indicator of future performance. Preventative actions begin with prescreening job applicants by validating work experience and education, conducting criminal background checks, and performing credit checks (Marquet, 2017; Young, 2014). According to ACFE (2016), approximately half of victim organizations utilized a background check when the perpetrator was employed. In 11% of the instances, the background check specified at least one red flag, such as prior criminal activity, employment issues, or financial concerns. Unfortunately, all of these organizations disregarded some noticeable issues. Biegelman and Bartow (2012), Brody et al. (2015), and Glodstein (2015) reported that a background check might include the following components: employment history,

including nature and length of service; education and professional licenses; personal references; criminal and credit history; medical history; and use of social media. Albrecht et al. (2006) found approximately 95% of fraud instances were caused by financial pressures, such as living beyond one's means, financial losses, and increased debt; therefore, financial background checks are also important sources of information. All of the participants indicated they confirmed prospective employees' employment history. Brody et al. (2015) recommended that prospective employers specifically ask if they would re-hire the applicant rather than only confirm employment dates. By conducting a diligent investigation into the applicants' employment history, employers should unearth any ethical concerns. Employers must utilize all means possible to make the best employment decisions.

The U.S. Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) prepared a publication to assist employers in conducting background checks on prospective employees. The report provided a list of topics that is legal to ask applicants. However, employers must be careful to comply with federal laws that protect prospective employees from discrimination. The EEOC included a description of discrimination based on religion; sex; color; race; national origin; disability; genetic information, which includes family medical history; and age, which includes individuals 40 years or older. Further, all background checks must be in compliance with the Fair Credit Reporting Act (FCRA), which is enforced by the FTC (Background checks: What employers need to know, 2014).

One participant described its detailed hiring process of prospective employees, which included a formal resume as well as at least two interviews and documentation. The participant explained, "We conduct a criminal background check as well as motor vehicle driving check. All of the facilities have zero tolerance against drugs, alcohol, bullying, cyberbullying, so our

hiring process is more thorough than most other places." Telephone reference checks included past employment and a determination as to whether the applicant was eligible for re-hire.

One participant had a human resources department which followed the equal opportunity guidelines for advertising a position. Further, the participant required a standard application form rather than accepting resumes to confirm that there were no discriminatory issues and received the same information from all applicants. There was a multiple interview process, which began with the HR interview. Next, applicants were interviewed by the manager, and ultimately by the CEO. This organization was unique in that after the first interview, applicants were required to take work-ready assessments through the Office of Workforce Development. The participant described the process, "They take a half-day assessment, which is related to problem solving, taking instruction, mathematics, spelling, and general work readiness as far as soft skills are concerned." Accounting applicants took an additional module related to computer skills. Drug screening was required for all prospective employees. Credit analysis was required for individuals involved with the financial functions of the business.

In the financial services business, the hiring process had two prongs: licensed and unlicensed hires. For the licensed employees who worked with client investors, the owners were actively involved with the entire process, from advertising the position to offering the job to the individual. Once the owners selected a person, the office manager then performed all of the background checks, fingerprinting, checking references, and drug testing. The broker also conducted background checks on licensed employees. For non-licensed employees, the human resources manager supervised the hiring process. The participant explained, "Since we are a small business, we usually like to do word of mouth first." Likewise, another business often used word of mouth and Facebook to advertise job openings. Since these organizations did not

have a formal human resource department, the supervising manager was active in the hiring process. For sales employees, the participant explained that prospective employees were typically given an evaluation, which is basically a personality test. Criminal background checks and driving records were essential for the drivers who delivered to security-sensitive military bases.

Payroll process. Wells (2004) and Williams and Kollar (2013) cited payroll fraud as an area that should be reviewed frequently. Actually, Stone (2016) reported that payroll fraud was reported twice as often in small businesses. Consequently, Glodstein (2015) recommended that owners regularly review payroll expense reports. All of the participants in the businesses reported that social security numbers were checked often to ensure there were no ghost employees. Bailey (2016) and Hall (2015) indicated that ghost employee schemes are common ruses used among fraudsters; however, this type of fraud is not as common in small organizations in which the owners are quite active. All of the participants indicated the hiring process was kept separate from the payroll process, with the exception of one business, in which both functions were performed by the owner. The payroll function was conducted internally in three businesses through a separate department. Employers also confirmed the number of hours that their employees worked. All of the small businesses used a time clock which registered the employees' hours worked. One business used face recognition software to sign in/sign out whereas the other organizations used either fingerprint ID or an employee number. One business used camera surveillance focused on the clock as the worker clocked in and out. All of the organizations stressed the importance of accurately recording hours worked. For example, one participant included a statement in the personnel manual that stipulated clocking in or out for another employee was a reason for immediate termination.

Job rotation/mandatory vacations. Approximately 20% of the organizations interviewed by the ACFE (2016) used job rotation and mandatory vacations as an internal control. Kapp and Heslop (2015) recommended that duties should be rotated periodically to make fraud concealment more difficult. The authors described several occasions in which fraudsters were caught because they refused to take vacations or went to work during difficult circumstances, such as returning to work soon after a surgical procedure. This "excessive dedication" to work raised red flags to potential fraudulent activities. Fraud risk indicators or red flags were defined by Gullkvist and Jokipii (2013) as "events, conditions, situational pressures, opportunities, or personal characteristics that may cause management employees to commit fraud on behalf of the company or for personal gain" (p. 45). Although the presence of red flags do not guarantee that fraud has occurred, it is an indication that internal controls should be investigated further to determine if any weaknesses and vulnerabilities are present. Neguriţă and Ionescu (2016) argued the importance of requiring mandatory vacations for employees who are in positions of significant control. None of the organizations in the study required mandatory vacations. One participant explained:

> [Employees] are rewarded in numerous ways, not just vacation, paid days off. When you move up the management scale, there are other incentives—bonus incentives, commission incentives, so there are ways to drive the employees to perform better as well as maintain the standards of the property other than offering and mandating vacations.

Since these are small businesses, the owners and/or managers would be aware if someone refused to take a vacation. If that were the situation, one participant explained, "We would require them to take a little bit of time, but that has not been an issue." As far as job rotation was concerned, none of the organizations had a formal job rotation policy. However, they had

employees who were trained in several areas so that duties can be accomplished even though some employees were absent. For example, one participant explained, "The accounts receivable person and the accounts payable person would not be off at the same time."

Separation of duties. Because of mistaken beliefs regarding fraud, small businesses sometimes find it challenging to institute effective internal controls. For example, Glodstein (2015), Klein (2015), and Stone (2016) described the challenges small businesses may have concerning separation of duties. They insisted that one individual should not have authority or responsibility over more than one part of a transaction. Kitching et al. (2013) and Neguriţă and Ionescu (2016) recommended there should be separation of duties between employees performing accounting, technology, and operating activities.

Ngwenya and Munyanyi (2015) and Howard (2015) elaborated that effective segregation means that one individual is never in a position to be responsible for initiating, approving, and recording a transaction. Moreover, Klein (2015) pointed out that employees should have limited authority over any transaction or accounting function. In fact, one participant indicated the process was quite detailed. For example, one employee was in charge of Accounts Payable. Then, both the accounting manager and CEO approved and initialed each check requested. Finally, one of the owners signed the check. Another participant indicated that one of the owners signed checks only for those invoices over a specified amount. Glodstein (2009) recommended that checks should require two signatures, and one person should not be responsible for both human resources and financial records. In another organization, only one signature was used on checks for large amounts since the check signor was an owner. Otherwise, two signature were required. The owners signed all checks in three of the businesses. In these instances, employees

were trained for more than one job so they could replace another person temporarily. In all of the businesses, job duties were separated.

Cash receipts and disbursements. Dull (2014) recommended that blank checks, cash and customer checks received should be kept secure until they are processed. Since one of the participants received a significant amount of cash on a daily basis, there was a multiple-step process for receiving and verifying cash:

> An [employee] will receive cash. Then, the night auditor reviews the balances and stores cash and checks in a safe. The morning person who audits also takes a look at that cash and then once it's deposited at the bank, it's reconciled by our CPA.

In addition, this participant installed security cameras over all of its registers. Although they did not receive as much cash, the other four small businesses also placed daily receipts in a safe, which were then re-counted and verified each morning prior to deposit. Another participant explained the process, "The accounting department folks rotate through locations and job duties."

All of the businesses studied restrictively endorsed checks that were received. For cash disbursements, such as refunds, voids, and discounts, there was a limited number of people in each organization who had the authority to process cash disbursements. These disbursements were reported on a daily report. One participant required authorization from two employees if the amount was over $100. In addition, one of the owners signed a refund check. In another business, the national broker/dealer provided cash disbursements to the clients rather than the local business. Two participants explained that when merchandise was returned, the businesses followed a three-part process. For example, one participant explained, "A driver picks up the

goods, the warehouse verifies that it was returned, and then the amount is credited by a customer service representative."

Purchases and inventory. Misappropriation of assets is one of the greatest sources of fraud for small businesses. According to the ACFE (2016) Report to the Nations, small businesses are often victims of misappropriation of assets which includes cash skimming (theft of cash prior to being recorded), cash larceny (theft of cash after it has been recorded), procurement fraud, and theft of inventory and other business assets. Actually, Stone (2016) reported that cash skimming and larceny were reported twice as often in small businesses. Of the small businesses studied, only one participant's business did not store inventory for sale. Whether it was cold storage or housekeeping supplies, eye glasses and contact lenses, building supplies, or office supplies and equipment, purchases were inventoried against purchase orders by a different employee from the person who placed the order, data were entered into the accounts payable account by a third employee, then the inventory was stored in a locked location, and re-inventoried weekly or monthly. All of the participants reported strictly professional relationships with vendors who were approved by an owner. However, since one participant had many vendors, including general office suppliers, pharmaceutical representatives, eyewear vendors, and eye testing equipment vendors, the manager reported a detailed purchasing policy that included a policy that stated "no employee is to receive any gifts of any monetary value." In fact, to aid in controlling purchases, supplies and inventory could only be purchased through its main office location. The participant clarified, "No doctor, even one of the physician owners, can attend a conference and make an order with a vendor." After explaining the process, the participant said, "Now that I say that out loud, I realize that we have a pretty good system."

Although securing blank checks may not be considered actual inventory, their security is very important. In fact, when asked if blank checks were secured, one participant laughingly replied, “They are now.”

Through the use of interviews, the researcher gained insightful information in regards to the internal controls implemented by the participants to mitigate employee fraud risk. Through an analysis of this information, the researcher addressed the research question and explored the conceptual framework. The internal controls included performing background checks during the hiring process, securing the payroll process, establishing job rotation and mandatory vacation policies, applying policies for separation of duties, designing a procedure for handling cash receipts and disbursements, and creating a process for making purchases and safeguarding inventory. For example, four of the businesses had a detailed hiring process which included the completion of a formal application form or formal resume, past employment and reference checks, drug testing, and criminal background checks. Two of the businesses had a separate human resources department. Three of the businesses processed payroll internally. None of the businesses required mandatory vacations nor participated in a formalized job rotation process. In all of the businesses, job duties were separated. Checks and cash received were secured and verified at night and the following morning prior to daily deposit in all of the businesses. In addition, purchases were inventoried upon receipt, compared with purchase orders, kept in secure localities, and re-inventoried weekly or monthly.

Information and Communication

It is vital for business organizations to provide and encourage effective communication with their employees. A participant elaborated:

> I pride myself in keeping my thumb on the pulse of the business by being in the dining room or at guest services upon checking-in in the lobby. In the hospitality industry, it's super important for me to have that communication with my guest service team.

Frazier (2016) emphasized the importance of communicating timely information so employees can perform their responsibilities appropriately as well as provide the means to communicate throughout the various levels of an organization. According to Pett et al. (2015), Principle 13 of COSO emphasizes the importance of organizations generating and using relevant information to maintain the effectiveness of internal controls. The authors explained that since organizations depend on having reliable information, they must assess changes in the information system to ensure the execution of control activities.

McNeal (2016) pointed out that active communication with employees creates an open-door policy and a culture of trust. The author also discussed the importance of providing a personnel manual for all employees, which included an organizational chart with the explanation that the employee's direct supervisor should be the first person to go to with a concern. However, the policy should also allow employees to take concerns to other levels or to the human resource department. Furthermore, Henry (2016) emphasized the importance of including a written code of conduct that provides guidelines to help employees conduct themselves in accordance with the businesses' primary values and ethical standards. Oseifuah and Gyekye (2013) explained that information and communication connect all elements of the COSO framework and are the means by which employees are made aware of internal controls and management's commitment to an anti-fraud climate. According to McNeal (2016), a written personnel manual should include the organization's mission statement, core values, and all company policies and practices. Providing a detailed personnel manual and offering routine

employee training are two of the best ways to provide information to and communicate with employees.

Personnel manual. One participant provided a personnel manual that explained the level of service expected of its employees as well as listed acts that would result in immediate termination for the first offense. The participant stated, "There's a lot of knowledge in the industry that we are in. Consequently, the organization also has a 'service training manual, that is another 70 pages that talks about the 'would you likes' versus the 'do you wants.'" Since this small business also included restaurants, the manual included policies for unauthorized eating and drinking, bag check, general rules of safety, procedure to report accidents, and telephone and social media usage. Beauprie (2015) specified that employers should warn employees of the risk of using social media websites. Another participant provided a document that described the two purposes of the personnel manual: (a) to protect the business, and (b) to protect the employee. The personnel manual included the mission statement; code of conduct; workplace procedures; employee benefits; policies for computer use, leave of absence, substance abuse, smoking, vehicle usage, return and care for company equipment; discipline; and termination. Another participant also provided a basic personnel manual; however, the manual was not as detailed since it did not include all of the items recommended for a good personnel manual, such as the topics listed in the manuals provided by the two participants mentioned previously. One business did not offer a personnel manual for its employees. The business provided a written explanation of duties for its supply drivers, which included a clarification of duties, personal appearance, vehicle maintenance, and delivery expectations. The participant emphasized the importance of drivers maintaining their professionalism because "the company truck is the greatest advertisement that we have."

Employee training. Employee training is one of the most important ways to develop employees' skills and be proactive about fraud concerns. Biegelman and Bartow (2012) advocated that fraud awareness training should include the following aspects: definition of fraud; the negative effect fraud has on organizational profits and employees' lives; examples of various types of fraud that could be perpetrated against a company; what can be done to stop fraudulent acts; and what to do if an employee suspects fraud. Likewise, Oseifuah and Gyekye (2013) highlighted that employees must understand their role in the internal control system and how their individual duties relate to other people's work. Further, according to Simha and Satyanarayan (2016), all employees should accept responsibility for detecting fraud. Biegelman and Bartow (2012) pointed out that a well-designed reporting system will fail without employee training.

One participant explained that "there is a lot of ethics and anti-fraud training required." Although this training was only required for licensed employees, this organization also provided that training to non-licensed employees. The participant elaborated, "The local training is more confidentiality training. For example, we are quite concerned with on-line security. But, we offer the same ethics and anti-fraud training." Three participants offered training that would improve job performance. Another participant took a different approach. The business did not have any type of training program. The participant explained the organization's philosophy: "I believe in setting the example by what you do and how you act. They know that I'm an ethical person, and I'm not going to do business with someone who's not. It trickles down." Small business owners cannot assume that employees know the requirements of a job and what is expected of them without thorough training, which also includes ethics and anti-fraud training.

The researcher posed interview questions to owners and/or managers to determine how small businesses in central Louisiana apply information and communication internal controls. The small businesses in this study exhibited strong internal controls that mitigated employee fraud risk. For example, one business owner and/or manager provided a detailed procedures manual as well as a training manual for its employees. Three businesses provided employee manuals, with varying degrees of detailed information. One business did not provide an employee manual. Three participants offered training that would help the employees better perform their jobs. One participant did not offer any type of employee training.

Monitoring

Monitoring is defined by Wilkins and Hann (2014) as performing assessments to determine whether the five components of internal controls are present and effective. Ngenya and Munyanyi (2015) defined internal controls as the collection of policies and procedures that are developed and implemented to advance efficiency, support laws and regulations, and foster accuracy in accounting procedures. Monitoring is an important element of the conceptual framework to assess and minimize the opportunities for fraudsters to perform fraudulent activities. There are numerous models that aid forensic accountants and auditors in helping their clients understand how to prevent fraud in their organizations. Cressey (1950) formulated the fraud triangle, in which he hypothesized that three components must be present for people to commit fraud: pressure (incentive), opportunity, and rationalization. Of these three elements, business owners and/or managers have the ability to minimize opportunity through the use of effective internal controls. Further, Trompeter et al. (2013) stressed the fraud triangle represents the actions of the fraudster prior to committing the fraud. The authors explained that during this time, the perpetrator assesses the number of anti-fraud measures in place and then determines if

he/she could successfully commit and conceal the fraud. Cressey's research has served as a basis to further develop the fraud framework, which aides in fraud prevention and detection. Similarly, Cohen and Felson (1979) proposed the routine activities theory (RAT) which centers on circumstances in which perpetrators carry out intentional criminal acts to explain the element of opportunity in the fraud triangle. Additionally, Argun and Dağlar (2016) pointed out the elements necessary to commit fraud include a motivated perpetrator who has an opportunity to execute a crime. Likewise, Trompeter et al. (2013) emphasized the importance of reducing or eliminating the opportunity for fraud by increasing internal controls, emphasizing the organization's culture by stressing an ethical tone at the top, and looking for red flags. They underscored these factors significantly reduce the opportunity for employee fraud. By understanding the opportunities that small businesses may unknowingly present to commit dishonest acts, business owners and/or managers can initiate internal controls that can reduce the potential for fraud. Monitoring is an important aspect of fraud prevention and is the primary method of assessing the effectiveness of the organization's internal controls.

COSO's *Guidance on Monitoring Internal Control Systems* (2009) stipulated two fundamental principles of the monitoring component of the COSO model. First is the premise that ongoing and/or separate evaluations will help owners and/or managers determine whether the other components of internal control continue to function. Second, internal control deficiencies are identified and communicated in a timely manner to those persons responsible for taking corrective action. On-going monitoring activities include continuously monitoring customer complaints and evaluating the organization's compliance with applicable laws and regulations. Businesses should also conduct separate evaluations, such as surprise audits. As

part of monitoring, businesses should take corrective action to adapt to changes that have been identified during the process.

Monitoring customer complaints. At first glance, one might wonder about the importance of monitoring customer complaints. Actually, the ACFE *Report to the Nations* (2016) indicated that 40% of the fraud tips received were made from nonemployees, such as customers and suppliers. For example, a customer who reports receiving a notice of nonpayment after an invoice was paid might tip off the manager that an employee had directed the customer's payment to a personal account. One participant created an anti-fraud climate by authorizing supervisors, service team, and front desk staff the permission to immediately handle customer concerns. In another business, patients and vendor complaints were handled by its human resource/marketing department. Another participant indicated that any complaint that was reported to the owner had to be reported to and handled by its broker/dealer as per industry standards. The participant elaborated:

> That's purely from the investment side. If there was a complaint about something … that's more of an internal, interoffice thing, then that would go to one of the owners. In a way, we're running two different businesses, the investment business and then the business of the business.

One participant reported that customer complaints were screened before being sent to the owner. After discussing this policy with the researcher, the participant concluded that the business needed further research to determine whether this policy was effective. In another business, the participant handled all complaints personally. Organizations should continually be monitoring customer concerns to potentially identify fraud risk.

Surprise audits. Although the ACFE report indicates that surprise audits are one of the least anti-fraud controls methods used, Murphy and Free (2016) noted it is one of the most effective ways to reduce the overall loss due to fraud. In addition, Camilo and Grimaldos (2014) argued that independence is a necessity when conducting audits that are objective. One participant had an internal accounting department which utilized the services of a local CPA firm to provide monthly review and oversight of the financial records. The owners preferred a monthly rather than an annual audit. In addition, the CPA firm conducted surprise audits. In another business, the person who was responsible for internal compliance conducted audits. Annually, the participant used these documents to prepare an industry-standard report. The business had an annual financial audit conducted by a CPA firm as far as the local business operations were concerned. Another participant had the most thorough surprise audit method. Periodically, the CPA logged on remotely and reviewed balance sheets and profit and loss statements. In addition, the CPA went to the business site and requested physical cash out receipts from the restaurants and reconciled them against the daily reporting performed through its financial software. This process audited the general manager as well as the other employees. Two other participants had a CPA firm that regularly reviewed their financial statements. However, they did not conduct surprise audits.

Managers should take advantage of using technology to assist in monitoring activities (Laxman et al., 2014). Three participants used comprehensive software to record their inventory. Moreover, Beach and Schiefellxin (2014) reiterated the importance of using technology to monitor data. The authors explained that fraudulent activities can be discovered through unconventional methods, such as email, telephone logs and calls, text messages, and social media. Unfortunately, many small business organizations do not take the time necessary to

monitor these types of data and are concerned with legal ramifications of putting employees' privacy at risk. Most legal issues regarding privacy can be avoided if the policies are reported in the personnel manual. Only one participant stipulated the social media usage policy. Organizations must determine if the benefits of data monitoring exceed the costs.

Adapting to changes. After internal controls have been monitored, the owner and/or manager must develop a plan to adapt to necessary changes. One participant explained that extensive changes had been made in the areas of the personnel manual and employee training. When the participant began working in this small business several years ago, he wrote the personnel manual as well as the service training manual. Prior to becoming the general manager, the participant worked as a bartender and recognized a lack of written procedures, expectations, and training. Another participant explained that after reviewing purchasing procedures:

> It became very complicated when satellite offices ordered their own supplies and inventory. Now, all purchases must be made at the main office. We do provide a credit card with a very small limit, like $200, for emergency supplies. This system has worked out a lot better.

One participant could not make changes to the investment part of the business because of industry requirements. Rather, the participant made changes in the operation of the business, as needed. For example, the participant revised its purchasing policy. Another participant made changes to remain in compliance with OSHA regulations and safety protocols, but made few changes with respect to office procedures or the financial aspect of the business. One participant adapted many changes in its product mix over the years to become a comprehensive office solutions company. However, the participant made few changes with regard to the business operations of the organization since the owner was predominately in charge of the various

aspects of business procedures. Continuous monitoring is essential to the viability, sustainability, and growth of these organizations.

The researcher addressed the central research question about internal controls, in regard to, monitoring by asking questions about handling customer complaints, conducting surprise audits, and adapting to changes. In all of the businesses, customer concerns were handled promptly by the owner and/or manager or a designated employee. Each of the small business organizations used local CPA firms that conducted surprise audits. After internal controls were monitored, all of the owners and/or managers developed a plan to adapt to necessary changes. Through these examples, the participants in this study demonstrated effective monitoring internal controls, which mitigated employee fraud risk.

Summary of Findings

This study provided the researcher with insight into the effectiveness of internal controls used in selected small businesses in central Louisiana and their impact on mitigating employee fraud risk. Interview questions concerning the control environment included topics on anti-fraud culture, owner and/or manager involvement, and availability of an ethics hotline. The owners and/or managers demonstrated their ethical values by vetting and selecting ethical vendors. All of the owners of the small businesses were very involved with the decision-making processes of the businesses. Although none of the businesses offered a formal ethics hotline, most of the owners provided personal, non-listed cell numbers for their employees. One organization held quarterly, one-on-one interviews in which the owner and/or manager asked if the employee had observed a fraudulent activity the employee wanted to report. The type of risk management assessment used in each company was dependent upon the type of industry. For example, in industries that required government regulations, the participants were concerned with

compliance assessment. The control activities portion of the interviews included a variety of topics such as obtaining background checks during the hiring process, securing the payroll process, establishing job rotation and mandatory vacation policies, applying policies for separation of duties, designing a procedure for handling cash receipts and disbursements, and creating a process for making purchases and safeguarding inventory. The hiring process varied in the five businesses. Two of the businesses had a separate human resources department. Four of the five organizations utilized a detailed process which included the completion of a formal resume or application form, checking past employment references, drug testing, criminal background check, and credit analysis, if the prospective employee would be working in the accounting department. Three of the businesses processed payroll internally whereas two organizations processed payroll using an external organization. None of the businesses required mandatory vacations nor participated in a formalized job rotation process; however, employees were trained for more than one job so they could replace other employees temporarily. In all of the businesses, job duties were separated. Although the majority of the small businesses studied did not handle a significant amount cash, checks and cash received was secured and verified at night and the following morning prior to daily deposit. Purchases were inventoried upon receipt, matched against purchase orders, kept in secure locations, and re-inventoried weekly or monthly. The information and communication varied among the businesses, ranging from offering a detailed employee manual and annual ethics and anti-fraud training to not providing a manual or any training for its employees. Monitoring organizations consisted of handling customer complaints, conducting surprise audits, and adapting to changes. Customer complaints were handled promptly by the owner and/or manager or a designated employee. Surprise audits were another way to monitor an organization. Each of the small business organizations used local

CPA firms, with three organizations conducting surprise audits. After internal controls were monitored, the owner and/or manager developed a plan to adapt to necessary changes. Some of these changes were made in the areas of the personnel manual, employee training, and the purchasing process. After the completion of this study, the researcher gained a greater understanding of the current practices of the internal control systems of selected small businesses, explored the effectiveness of their systems, and assisted the owner and/or manager develop a plan to improve their internal controls which could minimize fraud risk.

Applications to Professional Practice

The findings of this study addressed the central research question: "How do small businesses in Central Louisiana apply internal controls to mitigate employee fraud risk?" Further, the sub-question was "How do these small businesses meet the standards established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which included five elements: control environment, risk assessment, control activities, information and communication, and monitoring?" This sub-section included a comprehensive discussion on the applicability of the findings with respect to internal controls in small businesses and their impact on employee fraud. Specifically, *how* and *why* the findings were relevant to small businesses and their instituting internal controls to minimize fraud risk.

COSO (2013) defined internal controls as the procedures directed by an organization's board of directors, management, and/or employees which have been established to promote the achievement of organizational objectives. The Treadway Commission explained that internal control involves everything that controls risks to an organization's operational efficiency and effectiveness, accurate financial reporting, and compliance with regulations and laws. Dimitrijevic et al. (2015) described internal control as not a single event, but a series of activities

that evaluate an organization's outcomes in comparison to its goals. Based on the findings of this study, the researcher highlighted several themes of best practices of internal controls.

Control Environment

An organization's control environment sets the tone of the organization. Rae et al. (2017) explained the control environment forms the foundation for the other four components in the COSO model. Since all of the principles included aspects of integrity, control environment may also be considered to be the ethical environment of an organization. Therefore, Wilkins and Haun (2014) emphasized the importance of owners and/or managers creating an anti-fraud tone at the top. Patelli and Pedrini (2015) defined tone at the top as an atmosphere created by owners, board of directors, or chief executive officers. According to Henry (2016), the tone at the top of an organization has a significant effect on the probability and frequency of fraud. Murphy and Free (2016) and Wilkins and Haun (2014) described how the tone at the top is influenced by management's integrity and ethical values. The authors explained that when management encourages high ethical standards, the organization is less likely to be vulnerable to fraudulent activities.

Anti-fraud training. One way to assist in creating an anti-fraud tone at the top is by conducting anti-fraud training for its employees. This training is the initial step in implementing a fraud prevention and detection program. Training should include an explanation of how each employee's individual job duties relate to the work of other people and his/her role in the business' internal controls. In addition, the training should include examples of the kinds of fraud that might be committed against a small business in various industries and actions that can be taken to prevent fraudulent acts. The training should be used to educate employees of their responsibility in detecting internal control weaknesses and fraud occurrences. Also, several

authors (Glodstein, 2009; Hrncir & Metts, 2012; Loria, 2015; Van Gent et al. 2013) indicated that perpetrators are usually longtime, trusted friends and co-workers. An anti-fraud program is also important in educating employees about fraud risk indicators or red flags. Gullkvist and Jokipii (2013) defined red flags as "events, conditions, situational pressures, opportunities, or personal characteristics that may cause management employees to commit fraud on behalf of the company or for personal gain" (p. 45). Red flags do not guarantee that fraud has occurred; however, they are an indication that internal controls should be evaluated to determine if there are any weaknesses and if those vulnerabilities are being exploited.

Written code of conduct. Another way to establish an anti-fraud tone at the top is by providing employees with a written code of conduct, which includes the organization's values. It cannot be assumed that all employees will know what is expected of them. A code of conduct should be included in the personnel manual as well as emphasized in employee training. In fact, McNeal (2016) stressed that all personnel manuals should include the organization's mission statement and its core values. Likewise, Henry (2016) emphasized that a written code of conduct provides employees with the knowledge of the ethical values of the organization, the skills necessary to detect fraud, and the training about the actions to take when fraud is alleged. In addition, Ebberts (2015) noted the Ethics Research Center, which is devoted to the advancement of high ethical standards and practices, found that ethics awareness was an invaluable asset to businesses. In fact, the author reported that misconduct increased from 55% to 83% for those organizations that did not have a strong ethics program.

Another way to establish an ethical, anti-fraud tone at the top is by actively inquiring about possible fraudulent activities. For example, an organization could ask employees specifically if they are aware of any fraudulent activity or anything that should be reported to

management. These one-on-one interviews could also be included in routine performance evaluations, which could include the employees' participation in an organization's anti-fraud policies and procedures.

Risk Assessment

All business organizations, regardless of size, face both internal and external risks. Frazier (2016) stressed the importance of determining organizational objectives prior to risk assessment so risks can be identified and analyzed in accordance with the business' mission and goals. It is important to evaluate potential fraud and determine appropriate means to respond to significant fraud risk. Wilkins and Haun (2014) indicated that fraud assessment concerns minimizing risks as well as managing them. One way to assess risk is by establishing a Compliance and Risk Management Department or designate an employee responsible for ensuring compliance and assessing risk. Depending upon their industry, small businesses may need to be in compliance with HIPAA (Health Insurance Portability and Accountability Act) and OSHA (Occupational Safety and Health Administration of the United States Department of Labor) regulations.

Control Activities

Businesses must establish policies and procedures that govern day-to-day activities (Wilkins & Haun, 2014). In addition, Henry (2016) asserted that control activities associated with fraud prevention refer to the policies and procedures of an organization, including the hiring and onboarding process; approval processes and authorization levels; security of assets; and the segregation of duties.

Hiring and onboarding process. Past performance is an excellent method of predicting future performance. Preventative actions begin with prescreening job applicants by validating

work experience and education, conducting criminal background checks, and performing credit checks, particularly for those prospective employees who are involved in the financial aspect of the business (Marquet, 2017; Young, 2014). Biegelman and Bartow (2012), Brody et al. (2015), and Glodstein (2015) recommended that a background check might include the following components: employment history, including nature and length of service; education and professional licenses; personal references; criminal and credit history; medical history; and use of social media. Also, Brody et al. (2015) advised that prospective employers specifically ask if they would re-hire the applicant. Some employers are reluctant to conduct background checks because they fear they will be in violation of a law. Therefore, the U.S. Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) prepared a publication to assist employers in conducting background checks on prospective employees, which includes a list of topics that is legal to ask applicants. Of course, employers must be careful to comply with federal laws that protect prospective employees from discrimination based on religion; sex; color; race; national origin; disability; genetic information, which includes family medical history; and age, which includes individuals 40 years or older. All background checks must be in compliance with the Fair Credit Reporting Act (FCRA), which is enforced by the FTC (Background checks: What employers need to know, 2014). After conducting a diligent investigation into the applicants' backgrounds, prospective employers should discover most concerns. Employers must use all means available to make the best employment decisions.

Approval processes and authorization levels. Owners and/or managers should ensure that transactions are approved and executed only by employees acting within the scope of their authority. By allowing only specific individuals to authorize certain types of transactions, a layer

of responsibility can be added to ensure the accounting records are accurate and properly reflect the financial conditions of an organization. For example, requiring approval for large payments and expenses can prevent unscrupulous employees from making large fraudulent transactions (Ingram, 2018).

Security of assets. Kramer (2015) found that asset misappropriation is the most common type of employee fraud. Therefore, the researcher recommends that purchases be inventoried upon receipt, matched against purchase orders, kept in secure locations, and re-inventoried weekly or monthly. Bugariu (2016) pointed out that security and strict access to cash, equipment, and inventory should reduce the risk of loss or unauthorized use. In addition, Bugariu recommended the level of security of the assets should be based on the vulnerability of the items being secured. In other words, the probability of loss and the possible impact should a loss occur should be taken into consideration when assets are being secured.

Separation of duties. Some small businesses sometimes find it challenging to institute effective internal controls, such as separation of duties (Glodstein, 2015; Klein, 2015). Further, Ngwenya and Munyanyi (2015) and Howard (2015) elaborated that effective segregation means that one individual is never in a position to be responsible for initiating, approving, and recording a transaction. Separation of duties is necessary to reduce the opportunity to commit and conceal errors and/or perpetrate fraud. Glodstein (2009) recommended that checks should require two signatures, and one person should not be responsible for both human resources and financial records.

Information and Communication

Oseifuah and Gyekye (2013) pointed out that information and communication connect all elements of the COSO framework and are the means by which employees are made aware of

internal controls and management's commitment to an anti-fraud climate. In addition, Frazier (2016) stressed the importance of communicating timely information so that employees can perform their duties appropriately. Further, McNeal (2016) explained that active communication with employees creates an open-door policy and a culture of trust. One way to communicate with employees is by providing a personnel manual for all employees. A personnel manual protects the business as well as protects the employee. According to McNeal (2016), a written personnel manual should include the organization's mission statement; code of conduct; workplace procedures; employee benefits; policies for computer use, leave of absence, substance abuse, smoking, vehicle usage, return and care for company equipment; discipline; and termination.

Monitoring

Wilkins and Hann (2014) defined monitoring as performing assessments to determine whether the other four components of internal controls are present and effective. Monitoring is an important element of the conceptual framework to assess and minimize the opportunities for fraudsters to perform fraudulent activities. According to COSO's Guidance on Monitoring Internal Control Systems (2009), there are two principles of the monitoring component of the COSO model. The first supposition is that monitoring is ongoing and/or separate evaluations that help owners and/or managers determine if the other components of internal controls continue to function. Second, internal control deficiencies are identified and communicated in a timely manner to those persons who are responsible for taking corrective action. One way to monitor activities is to conduct unscheduled assessments, such as surprise audits. Although the ACFE report indicated that surprise audits are one of the least anti-fraud controls methods used, Murphy and Free (2016) documented surprise audits are one of the most effective ways to reduce

the overall loss due to employee fraud. In addition, Camilo and Grimaldos (2014) stipulated that independence is a necessity when conducting surprise audits.

Biblical Framework Implications

Fraud is a not an accounting problem; it is a human problem. Fraud is a criminal deception with the intention of deceiving others for personal financial gain (Fraud, 2018). People were encouraged to be ethical in their business dealing when Moses stated in Leviticus 19:11: "You shall not steal; you shall not deal falsely; you shall not lie to one another." Van Duzer (2010) described how employees should conduct themselves to demonstrate God's character. He emphasized the importance of employees consistently demonstrating integrity. Van Duzer (2010) explained employees should work diligently by giving an honest day's work for an honest day's wage. People were encouraged in Proverbs 6:6-11 to "go to the ant" to "consider its ways" as a reminder to not be a sluggard. Likewise, people were reminded in Proverbs 10: 4 that "lazy hands make for poverty, but diligent hands bring wealth." Employees should be diligent at "whatever [they] do, work at it with all of [their] hearts, as working for the Lord, not human masters" (Colossians 3:23). Employees should work for what they have, not resort to fraudulent acts. Regardless of an employees' level in a business, they can demonstrate ethical character which honors God. Van Duzer (2010) also pointed out that businesses must practice sustainability. In the case of investors or small business owners, the concept of sustainability means stakeholders should receive a reasonable return on their investment. The sustainability of an organization comes into question when fraud exists. Van Duzer (2010) described God's purpose for business, which is to serve others by providing goods or services needed in the community as well as to express employees' God-given abilities through meaningful, honest work experiences. Further, Keller (2012) reiterated that without meaningful

work, individuals often lack the opportunities to flourish physically, emotionally, and spiritually. Dorothy Sayers summarized the importance of work: "[It] is that work is not, primarily, a thing one does to live, but the thing one lives to do" (Keller, 2012, p. 38).

Employee fraud affects the fraudster, business organization, and society as a whole. If an individual commits fraud, the fraudster and his/her family suffer the consequences. Joshua described the account of Achan's sin of stealing and lying. Achan explained in Joshua 7:21: "When I saw in the plunder a beautiful robe from Babylonia, two hundred shekels of silver and a bar of gold weighing fifty shekels, I coveted them and took them." As a result of his theft, verses 24-25 described the consequences of his sin:

> Then Joshua, together with all Israel, took Achan son of Zerah, the silver, the robe, the gold bar, his sons and daughters, his cattle, donkeys and sheep, his tent and all that he had, to the Valley of Achor. Joshua said, "Why have you brought this trouble on us? The Lord will bring trouble on you today." Then all Israel stoned him, and after they had stoned the rest, they burned them.

This story is a reminder that one person's actions affect others. In the case of fraud in an organization, the fraudster could be prosecuted, which, in turn, affects the entire family. Also, the business may receive a negative reputation, which could result in a financial loss for the owners, investors, and fellow employees. Ultimately, the business may declare bankruptcy, which could have a negative impact on the local economy. The gain a person might receive from fraud creates a downward spiral.

Scripture advises us to be honest with God. Fraud is not being honest with humanity or God. In Acts 5:1-11, Luke discussed the deaths of Ananias and Sapphira, his wife. After they had sold a parcel of land, they told Peter they had donated the proceeds to the church; however,

they had not. Meyer (n.d.) wrote they "had selfishly embezzled the remainder for themselves" (para. 1). Also, John Stott (1994), an English Anglican priest and leader of the worldwide evangelical movement, wrote:

> Ananias and Sapphira were not so much misers as they were thieves. They wanted the credit and the prestige for sacrificial generosity, without the inconvenience of it. So, in order to gain a reputation to which they had no right, they told a brazen lie. Their motive in giving was not to relieve the poor, but to fatten their own ego. (para. 2)

Based on the findings of this study, small business owners and/or managers must develop and implement internal controls to equip their organizations to better achieve God's purpose for business.

Field of Study Implications

The discipline of accounting is comprehensive. Three primary areas of accounting include public accounting, private accounting, and government/non-profit accounting. In each area, internal controls play a significant role. For example, in public accounting, compilations, reviews, and audits comprise significant policies and procedures related to the internal controls of an organization. In fact, the audit opinion specifically addresses internal controls. In private accounting, organizations can have internal auditors on staff whose duties include the development, implementation, and monitoring of internal controls. Government and non-profit organizations also use internal controls. Many grants and donor contributions may require reviewed or audited financial statements, which require an assessment of the organization's internal controls. Whether small businesses or large corporations, internal controls contribute significantly to the relevance and accuracy of financial data. Internal controls should be assessed to determine their impact on employee fraud.

Internal controls serve a critical role in safeguarding an organization's assets, which ultimately affect its fate. The purpose of the study was to gain greater understanding of current internal control practices of small businesses and explore the effectiveness of their systems, which could mitigate employee fraud risk. The results of this study may be used to assist small business owners and managers to become more knowledgeable in the development, implementation, and monitoring of effective internal controls so the potential for employee fraud risk can be minimized. Effective internal controls can improve an organization's financial stability, growth, and sustainability.

The implications of this study on accounting are three-fold: (1) explore the importance of developing and implementing effective internal controls to better achieve organizational goals and decrease the risk of employee fraud; (2) emphasize the importance of evaluating internal controls by applying the five components of the COSO model: control environment, risk assessment, control activities, information and communication, and monitoring; and (3) demonstrate the importance of conducting anti-fraud training.

Importance of internal controls. Verovska (2014) explained the aim of effective internal controls as being to improve the business's financial stability, create a competitive edge, and instill confidence in its owners and shareholders. Internal controls may be defined as a compilation of policies and procedures developed and implemented to foster efficiency, encourage accuracy in accounting procedures, uphold regulations, and inspire employees to attain organizational goals (Oseifuah & Gyekye, 2013; Jahmani et al., 2014; Ngwenya & Munyanyi, 2015. Further, Corns (1971) stated, "Controls protect weak people from temptation, strong people from opportunity, and innocent people from suspicion" (p. viii). According to Dimitrijevic et al. (2015), internal controls are a series of activities that evaluate an

organization's outcomes in comparison to its goals. Ngwenya and Munyanyi (2015) and COSO (2013) further clarified that internal controls govern both human and financial resources in an effort to monitor organizations to prevent fraudulent activities and promote realistic assurance concerning the achievement of organizational objectives.

Importance of evaluating internal controls by applying the COSO model. With the increase in the number of fraud perpetrators, business owners found it necessary to develop a model for assessing evaluating internal controls. Biegelman and Bartow (2012) explained that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 as a voluntary organization. Professional finance and accounting organizations including Financial Executives International, the American Institute of Certified Professional Accountants, the American Accounting Association, the Institute of Internal Auditors, and the Institute of Management Accountants were involved in the origination of COSO. In 1992, COSO constructed a model for assessing internal controls, which included five components: control environment, risk assessment, control activities, information and communication, and monitoring (Cotton et al., 2016). These elements should be assessed continuously, and weaknesses should be addressed in a timely manner.

Conducting anti-fraud training. Anti-fraud employee training is the initial step in implementing a successful fraud awareness, prevention, and detection program. Training should include a description of how each employee's individual duties relate to the work of other people as well as his/her role in exploring the business' internal controls. It should also be used to communicate to employees their responsibility in detecting internal control weaknesses and fraud occurrences. In addition, it is important to inform employees that perpetrators can be, and often are anyone, including trusted co-workers and friends. An anti-fraud program is also

important in educating employees about red flags or fraud risk indicators. Gullkvist and Jokipii (2013) defined red flags as "events, conditions, situational pressures, opportunities, or personal characteristics that may cause management employees to commit fraud on behalf of the company or for personal gain" (p. 45). The presence of red flags does not guarantee that fraud has occurred; however, it is an indication that internal controls should be evaluated to determine if there are any weaknesses and if those vulnerabilities are being exploited. Although most accountants are familiar with ways to identify altered accounting data, they also need to understand the human elements involved, such as recognizing fraud risk indicators.

This research was vital to achieving a better understanding of current business practices concerning how effective internal controls can minimize fraud risk in small businesses. Through the application of these best practices, small businesses can enhance the opportunity to accomplish their strategic, operational, financial, and compliance objectives.

Recommendations for Action

Based on the findings of this study, the researcher identified six recommendations for action that small business owners and/or managers should consider to improve the internal controls in their businesses, which could mitigate employee fraud risk. These recommendations include establishing internal controls, addressing personnel issues, conducting anti-fraud training, revising personnel manuals, assessing risk, and monitoring COSO standards.

Establishing Internal Controls

Owners of small businesses need professional business counseling to plan, launch, manage, and grow their businesses. The Small Business Administration (www.sba.gov) is one source that is available to small business owners and/or managers. In addition, the local Central Louisiana chapter of the Society of Louisiana CPAs (www.lcpa.org) can offer assistance in

setting up the best practices of internal controls. These organizations provide on-going training in various aspects of operating a successful organization including the identification and implementation of effective internal controls.

Addressing Personnel Issues

For assistance, in developing or improving control activities related to personnel issues, the researcher recommends that small business owners and/or managers utilize resources available through the Society of Human Resource Management (SHRM), which can be located at www.shrm.org. For example, SHRM provides tools that assist in creating or revising personnel manuals, which includes writing job descriptions and organizational policies. In addition, SHRM provides tools that assist with the entire interviewing process: screening and evaluating candidates; initial interview questions, managing the employee on-boarding and assimilation process, performance appraisals, and exit interview questions. Resources are also available concerning "Starting an HR Department from the Ground Up," which can assist owners and/or managers focus on improving their internal controls relating to personnel issues.

Conducting Anti-fraud Training

Anti-fraud training is fundamental for instituting a successful fraud awareness and prevention program. Kramer (2015) summarized it best with "Blind trust is not an internal control" (p. 12). Anti-fraud employee training is the initial step in implementing a fraud prevention and detection program. The small businesses studied in this effort offered more training concerning governmental compliance rather than anti-fraud training. Therefore, the researcher recommends that small businesses develop comprehensive anti-fraud training that includes an explanation of how each employee's individual job duties relate to the work of other people and his/her role in the business' internal controls. Individuals who are planning training

seminars may want to refer to *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance* (Biegelman & Bartow, 2012). This book covers topics such as training, internal controls, financial statement fraud, internal and external fraud schemes, and the ACFE fraud prevention checklist. The training should include examples of the types of fraud that might be perpetrated against a particular business and actions that can be taken to prevent fraudulent acts. The training should be used to inform employees of their responsibility in detecting internal control weaknesses and fraud occurrences. In addition, it is important to inform employees that perpetrators can be, and often are anyone, including trusted friends and co-workers. An anti-fraud program is also important in educating employees about fraud risk indicators or red flags. Gullkvist and Jokipii (2013) defined red flags as "events, conditions, situational pressures, opportunities, or personal characteristics that may cause management employees to commit fraud on behalf of the company or for personal gain" (p. 45). Although the presence of red flags does not guarantee that fraud has occurred, it is an indication that internal controls should be investigated to determine if there are any weaknesses and if those vulnerabilities are being exploited.

The Association of Certified Fraud Examiners (ACFE), which can be located at www.acfe.com, prepares a bi-annual *Report to the Nations*, which is the largest global study on occupational fraud. Data are collected from 125 countries that represent 23 major industry categories. ACFE explores the costs, schemes, victims, and perpetrators of fraud. By providing this information to their employees through training seminars, owners and/or managers will equip their employees with a better understanding of fraud. In addition to the *Report to the Nations*, ACFE also provides self-study CPE classes. Other organizations also offer CPE courses, such as The CPE Store (www.cpestore.com). This organization offers training in such

topics as COSO internal controls, forensic accounting and fraud, profiling the fraudster, and accounting controls. It is much more effective and economical for business organizations to participate in fraud prevention activities rather than have to utilize fraud detection methods (Singh et al., 2013).

Revising Personnel Manuals

Small business owners and/or managers may need to revise their organizations' employee manuals since these guides are essential in preparing employees to recognize and detect fraud. Written, comprehensive personnel manuals aid owners and/or managers in communicating expectations to their employees. McNeal (2016) explained that a written personnel manual should include the organization's mission statement, core values, and all company policies and practices. In addition, Henry (2016) emphasized the importance of including a written code of conduct that provides guidelines to help employees conduct themselves in accordance with the businesses' ethical values and standards. Miller (2014) recommended that owners and/or managers require all employees to sign an acknowledgment form that would be dated and kept on file indicating that the employee has received, read, and understood the personnel manual. The author pointed out that this documentation would be helpful to employers if there was ever a dispute or disciplinary issue. The results of this study indicated that, while the majority of the participating organizations currently provide their employees with personnel manuals, revisions may be necessary to ensure that the manuals are more comprehensive and inclusive of essential elements. Owners and/or managers can access the National Federation of Independent Business (NFIB), America's leading small business association, for G*uidelines on How to Write a Great Employee Handbook* (www.nfib.com/content/resources/labor/how-to-write-a-great-employee-handbook/). Personnel manuals enable the employer to explain the duties that need to be

performed and provide employees with realistic expectations, including effective internal controls.

Assessing Risk

Risk assessment, one of the components of the COSO model, is vital for organizations to manage risks effectively in order to maintain operations and accomplish their business objectives. However, risk assessment can be a challenge for small business owners and/or managers. To assist in this endeavor, COSO published *Embracing Risk Management: Practical Approaches to Getting Started* (2011). Risk assessment follows identification of an event, but precedes a response to the risk. Its purpose is to assess and prioritize the risks and then focus on the response to the risks. In addition, COSO published *Risk Assess in Practice* (2012), which covers the following topics: describing the risk assessment process, developing assessment criteria, assessing risks, assessing risk interactions, and prioritizing risks. Small businesses owners and/or managers should utilize an effective assortment of risk assessments to reduce the risk of employee fraud.

Monitoring COSO Standards

Monitoring is an integral part of internal controls. Owners and/or managers should seek resources to improve their ability to monitor the organization. The COSO Board realized the assessment of internal control can be a time-consuming task. In an effort to make this process more effective and streamline the assessment process, COSO developed the COSO Internal Control Integrated Framework: Guidance on Monitoring Internal Control Systems (2009), which provides a discussion of the fundamentals of effective monitoring, the monitoring process, and which controls are "key controls." COSO's Monitoring Guidance is designed to assist owners

and/or managers as they improve the effectiveness of the monitoring process of the other four COSO standards.

Who may be impacted by the study. These six recommendations can provide valuable resources that will assist small business owners, managers, and employees in the prevention, mitigation, and detection of employee fraud. Likewise, local organizations who assist prospective entrepreneurs as well as existing owners and/or managers would benefit from the findings of this study. For example, in the researcher's geographic area, the Louisiana Small Business Development Center (LSBDC) Northwest and Central Region are located in Natchitoches, Louisiana, and offers free business consulting services, such as industry-specific courses and technology training, to both new and existing businesses.

Other researchers who are studying internal controls, specifically in small business organizations, would also benefit from the findings of this study. Since a limited number of studies on the internal controls of small businesses exists, this study may encourage other researchers to conduct further research on this topic.

Dissemination of findings. The researcher identified several methods to disseminate information to people affected in the Plan of Action.

(1) Coordinate with the Chamber of Commerce's incubator program to offer anti-fraud and internal control training sessions for prospective entrepreneurs, with an emphasis on minority small business owners.

(2) Coordinate with the local Chamber of Commerce to offer anti-fraud and internal control training sessions to its members who are interested in knowing how to better assess and improve their internal controls.

(3) Offer seminars to community leaders, such as bankers and CPAs who assist small business owners and/or managers in developing and implementing internal controls.

(4) Host a forum where business leaders with an expertise in this topic would serve as speakers and discuss internal controls and employee fraud.

(5) Publish articles and present at accounting conferences, such as the American Accounting Association, on the findings of this study and the importance of effective internal controls to mitigate employee fraud risk.

After the plan of action has been accomplished, owners, managers, employees, and prospective entrepreneurs may have a better understanding of internal controls and be able to develop and implement effective internal controls and assess and minimize potential employee fraud risk.

Recommendations for Further Study

Based on the findings of this study, it would be beneficial to conduct further exploration of the internal controls of small businesses. The researcher has three recommendations for further study. First, future studies could include an analysis based on the longevity of how long the organizations have been in business. For example, businesses could be divided into the following categories: 1-5 years; 6-10 years; 11-15 years; over 15 years. This might indicate a greater need for education in appropriate internal controls and in preventing and detecting employee fraud in younger organizations. Second, the researcher recommends that future researchers with an interest in internal controls and employee fraud study several small businesses within the same industry. The research from those studies could indicate which industries have better, more effective internal controls to minimize employee fraud. With this information, researchers could develop practitioner seminars and training to strengthen the

internal controls unique to a particular industry. Third, researchers could evaluate the internal controls of small non-profit organizations since there is limited research concerning the internal controls in these businesses. By conducting further studies, researchers can gain a greater understanding of the current practices of the internal control systems in comparison to anti-fraud activities in small businesses.

Reflections

Research Process

In a qualitative study, the researcher serves as the primary instrument; therefore, it is imperative that the researcher reflect throughout the study. To avoid predisposition during the data collection phase, the researcher used the same criteria and wording for all participants. Then, after the interviews were meticulously transcribed, the researcher used respondent validation by allowing the participants to verify the accuracy of the transcripts. After the initial interview, the interviewer realized he had preconceived ideas concerning the level of internal controls used in small businesses. Based on the research described in the literature review, the interviewer assumed that the business owners who participated in this study would have limited involvement in the day-to-day operations and have no external audits. However, 100% of these business owners were actively involved in the organization, and 100% of the businesses utilized external accountants. Consequently, the researcher had a change in his thinking concerning the internal controls of small businesses that participated in this study.

After reflecting on the effectiveness of the questionnaire, the researcher also realized that revisions should be made. The first interview question should include a description of the small business, such as the organizational structure, growth or changes in the business, and the number of years it has been in existence. Also, it would be helpful to ask the respondent if the business

had ever been a victim of fraud; and, if so, to explain the event. This information would provide insight into the commitment of the business owner and/or manager concerning internal controls that could decrease employee fraud risk. In addition, while the researcher was organizing the data, he realized that redundant questions should be eliminated. To make analysis less complicated, individual questions should be aligned with the COSO model, ensuring that each question does fall under the various elements of the COSO model. Also, some sections, such as risk assessment and monitoring, should have additional questions that would provide clarity to the respondent in order to better understand specific areas in which to comment.

Biblical Principles

There is a direct correlation between the effectiveness of internal controls and fraud risk. Dishonest dealings are discussed frequently in the Bible. Fraud is stealing, taking something without permission. The Lord, through Moses, emphasized the need to be ethical in business transactions, "You shall not steal; you shall not deal falsely; you shall not lie to one another" (Leviticus 19:11, English Standard Version). Some fraudsters justify their actions by rationalizing that they are borrowing the money. However, Psalm 3:21 describes the person who borrows and does not repay as "wicked" but "blessed" when he/she "eat[s] the fruit of the labor of [his/her] hands (Psalm 128:2). In Ephesians 4:28, Paul stated "the thief must no longer steal. Instead, he must do honest work with his own hands, so that he has something to share with anyone in need." Unfortunately, not all individuals have the education and/or experience needed to obtain the position and salary that their preferred lifestyle would require. Consequently, some of them resort to employee fraud to fill the gap (Ruankaew, 2016). Although fraud cannot be completely eliminated, establishing internal controls can significantly reduce employee fraud risk.

Summary and Study Conclusions

Benjamin Franklin's (1735) axiom stated "An ounce of prevention is worth a pound of cure" can be appropriately applied to employee fraud. The purpose of this qualitative study was to gain greater understanding of the current practices of the internal control systems of small businesses and explore the effectiveness of their systems in comparison with anti-fraud activities recommended by forensic accountants.

The researcher selected five participants, based on the study's parameters: members of the Central Louisiana Regional Chamber of Commerce who had fewer than 100 employees. The objective of the interviews in this multi-case study was to gain greater understanding of the current practices of the internal control systems of selected small businesses and explore the effectiveness of their systems. Accordingly, the central research question was: "How do small businesses in central Louisiana apply internal controls to mitigate employee fraud risk?"

The researcher referred to elements of the conceptual framework to develop an interview guide for use in assessing and minimizing opportunities for fraudsters to perform fraudulent activities. One of the models that allows forensic accountants and auditors to help their clients understand how to prevent fraud in their organizations is Cressey's (1950) fraud triangle. Cressey (1950) hypothesized that three components must be present for people to commit fraud: pressure (incentive), opportunity, and rationalization. Of these three elements, business owners and/or managers have the ability to minimize opportunity through the use of effective internal controls. Further, Trompeter et al. (2013) explained the perpetrator assesses the number of anti-fraud measures in place and then determines if he/she could successfully commit and conceal the fraud prior to committing fraud.

The researcher consulted the Enterprise Risk Management (ERM) Integrated Framework and the International Organization for Standardization (ISO) in developing interview questions to address the central research question. McNally (2015) described the 2004 ERM as a complementary model to COSO's internal control framework. The International Organization for Standardization (2009) includes guidelines of risk management to assist businesses achieve their goals and identify threats of fraud risk.

The owner and/or manager from each small business participated in a 44-question, one-on-one, semi-structured interview with the researcher. The interview questions reflected the five components of the COSO (2013) model: control environment, risk assessment, control activities, information and communication, and monitoring.

Since the literature review in this study indicated that few internal controls are used in small business organizations, the results of this study were somewhat surprising. The participants in this study indicated their businesses used more internal controls than were depicted in the literature review. In addition, the researcher highlighted several themes of best practices of internal controls: anti-fraud training; written code of conduct; risk assessment; hiring and onboarding process; approval processes and authorization levels; separation of duties; information and communication; and monitoring. Anti-fraud training is the initial step in implementing a fraud prevention and detection program. Training should include an explanation of how each employee's individual job duties relate to the work of other people and his/her role in the business' internal controls. An anti-fraud tone at the top may be established by providing employees with a written code of conduct, which includes the organization's values. All businesses, regardless of size, face internal and external risks. Fraud assessment concerns minimizing risks as well as managing them. Businesses must establish policies and procedures

that govern day-to-day activities. Four control activities that are vital for the success of a business includes the hiring and onboarding process; approval processes and authorization levels; security of assets; and separation of duties. Information and communication connect all elements of the COSO model and are the means by which employees are made aware of internal controls. Monitoring is important to assess and minimize opportunities for perpetrators to conduct fraudulent activities.

The researcher made six recommendations for action to small business owners and/or managers to help achieve their organization's objectives: establishing internal controls; addressing personnel issues; conducting anti-fraud training; revising personnel manuals; assessing risk; and monitoring COSO standards. These recommendations provided specific tools that may assist a small business owner and/or manager in preventing, mitigating, and detecting employee fraud.

While many studies have been conducted on large business entities, this research fulfilled a need for studying the effect of internal controls on employee fraud in small businesses. Opportunities to commit fraud are available in all organizations. While owners and managers cannot control the incentives of fraudsters, they can reduce the opportunities for fraud to occur by engaging in strong internal controls.

References

Abdel-Khalik, A. R. (2014). Prospect theory prediction in the field: Risk seekers in settings of weak accounting controls. *Journal of Accounting Literature, 33*(1/2), 58-84.

Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences, 5*(4), 38-45. doi: 10.6007/IJARAFMS/v5-i4/1823

Agnew, R. (2015). Using General Strain Theory to explain crime in Asian Societies. *Asian Journal of Criminology, 10*(2), 131-147. doi: 10.107/s1147-014-9198-2

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2012). *Fraud examination*. Mason, OH: Cengage Learning.

Albrecht, W. S., Hill, N. C., & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. *Australian Accounting Review, 16*(1), 30-40. doi: 10.1111/j.1835-2561.2006.tb00323.x

American Institute of Certified Public Accountants (AICPA). (n.d.). *Audit Risk Assessment Tool and Guide*. New York, NY: American Institute of Certified Public Accountants, Inc.

American Institute of Certified Public Accountants (AICPA). (n.d.). *Managing the Business Risk of Fraud: A Practical Guide.* American Institute of Certified Public Accountants. 1-80. Retrieved from https://www.aicpa.org/InterestAreas/ForensicAndValuation /Resources/FraudPreventionDetectionResponse/DownloadableDocuments /managing_business_risk_fraud.pdf

Anand, V., Dacin, M. T., & Murphy, P. R. (2015). The continued need for diversity in fraud research. *Journal of Business Ethics, 131*(4), 751-755. doi: 10.1007/s10551-014-2494-z

Argun, U., & Dağlar, M. (2016). Examination of routine activities theory by the property crime. *International Journal of Human Sciences, 13*(1), 1188-1198. doi: 10.14687/ijhs.v13i1.3665

Association of Certified Fraud Examiners. (2016). *Report to the Nations on Occupational Fraud and Abuse,* 1-92. Retrieved from http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

Background checks: What employers need to know. (2014). *U.S. Equal Employment Opportunity Commission*. Retrieved from https://www.eeoc.gov/eeoc /publications/background_checks_employers.cfm

Bailey, J. A. (2016, June). Fraud and related-party transactions: Internal auditors can identify red flags and reduce the risk and impact of related-party fraud. *Internal Auditor*, *73*(3), 58-63.

Balsam, S., Jiang, W., & Lu, B. (2014). Equity incentives and internal control weaknesses. *Contemporary Accounting Review*, *31*(1), 178-201. doi: 10.1111/1911-3846.12018

Barrett, J. R. (2007). The researcher as instrument: Learning to conduct qualitative research through analyzing and interpreting a choral rehearsal. *Music Education Research, 9*(3), 41733.

Beach, C. S., & Schiefellxin, W. R. (2014, January). Unstructured data: How to implement an early warning system for hidden risks. *Journal of Accountancy*, *217*(1), 46-51.

Beauprie, A. (2015). The “Fake President” fraud. *Internal Auditor*, *72*(2), 25-27.

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177-186. doi: 10.1016/S0363-8111(97)90023-0

Biegelman, M. T., & Barlow, J. T. (2012). *Executive roadmap to fraud prevention and internal control: Creating a culture of compliance*. Hoboken, NJ: John Wiley & Sons, Inc.

Birt, L., Scott, S., & Cavers, D. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802-1811. doi: 10.1177/1049732316654870

Brody, R. G., Melendy, S. R., & Perri, F. S. (2012). Commentary from the American Accounting Association's 2011 annual meeting panel on emerging issues in fraud research. *Accounting Horizons*, *26*(3), 513-531. doi: 10.2308/acch-50175

Brody, R. G., Perri, F. S., & Van Buren, H. J. (2015). Further beyond the basic background check: Predicting future unethical behavior. *Business and Society Review*, *120*(4), 549-576. doi: 10.1111/basr.12074

Buckley, A. P. (2015). Using sequential mixed methods in enterprise policy evaluation: A pragmatic design choice? *Electronic Journal of Business Research Methods*, *13*(1), 16-26.

Bugariu, K. (2016, February). Internal controls and best practice. *AA Roundup*. 1-41. Retrieved from http://studylib.net/doc/11266139/internal-controls-and-best-practice-katarina-bugariu

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. doi: 10.2308/jmr-51471

Camilo, A., & Grimaldos, G. (2014). Maintaining our reputation. *Internal Auditor*, *71*(1), 72.

Campbell, L., Butler, J., & Raiborn, C. (2014). Minimizing fraud during a boom business cycle. *Management Accounting Quarterly*, *16*(1), 1-12.

Caufield, T., & Steckler, S. (2014, December). The five faces of procurement fraud, abuse, and noncompliance. *Contract Management,* 38-45. Retrieved from http://read.nxtbook.com /ncma/contractmanagement/december2014/thefivefacesofprocurement_feat.html

Cleary, M., Horsfall, J., & Hayter, M. (2014). Qualitative research: Quality results? *Journal of Advanced Nursing*, *70*(4), 711-713. doi: 10.1111/jan.12172

Cohen, L. E., & Felson, M. (1979). Social rates and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. doi: 10.2307/2094589

Cordoba-Pachon, J. R., & Loureiro-Koechlin, C. (2015). Online ethnography: A study of software developers and software development. *Baltic Journal of Management*, *10*(2), 188-202. doi: 10.1108/BJM-01-2014-0016

Corns, M. C. (1971). *How to Audit a Bank*. Boston, MA: Bankers Publishing Company.

COSO Embracing risk management: Practical approaches to getting started. (2011). 1-20. Retrieved from https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf

COSO Guidance on Monitoring Internal Control Systems. (2009). 1-10. Retrieved from https://www.coso.org/documents/COSO_Guidance_On_Monitoring_Intro_online1_002.pdf

COSO Internal Controls—Integrated Framework. (2013). 1-8. Retrieved from https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf

COSO Internal Control Integrated Framework: Guidance on Monitoring Internal Control Systems. (2009). 1-10. Retrieved from https://www.coso.org/Documents/COSO _Guidance_On_Monitoring_Intro_online1_002.pdf).

COSO Risk Assessment in Practice. (2012). 1-28. Retrieved from https://www.coso .org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf

Cotton, D. L., Johnigan, S., & Givarz, L. (2016, September). Fraud risk management guide: Executive summary. *Committee of Sponsoring Organizations of the Treadway Committee*, 1-14. Retrieved from 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. doi: 10.2307/2086606

Creswell, J. W. (2013). *Qualitative inquiry & research design: Choosing among five approaches*. Thousand Oaks, CA: Sage.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.

Creswell, J. W., Shope, R., Clark, V. L. P., & Green, D. O. (2006). How interpretive qualitative research extends mixed methods research. *Research in the Schools, 13*(1), 1-11.

Criminal law—Computer Fraud and Abuse Act—Ninth Circuit affirms conviction of a former employee who used another employee's password. (2016). *Harvard Business Review, 130*, 1265-1272. Retrieved from https://harvardlawreview.org/

Crouch, M., & McKenzie, H. (2006). The logic of small samples in interview-based qualitative research. *Social Science Information, 45*(4), 18. doi: 10.1177/0539018406069584

D'Aquila, J. (2013, October). COSO's Internal control—Integrated framework: Updating the original concepts for today's environment. *The CPA Journal, 83*(10), 22-29.

Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum, 37*, 29-39. doi: 10.1016/j.accfor.2012.09.003

DeVault, G. (2017, June). Establishing trustworthiness in qualitative research: What are qualitative research processes? *The Balance*. Retrieved from https://www.thebalance.com /establishing-trustworthiness-in-qualitative-research-2297042

Dilla, W. N., Harrison, A. J., Mennecke, B. E., & Janvrin, D. J. (2013). The assets are virtual but the behavior is real: An analysis of fraud in virtual worlds and its implications for the real world. *Journal of Information Systems*, *27*(2), 131-158. doi: 10.2308/isys-505771

Dimitrijevic, D., Milovanovic, N., & Stancic, V. (2015). The role of a company's internal control system in fraud prevention. *Financial Internet Quarterly, e-Finanse, 11*(3), 34-44. doi: 10.14636/1734-039X_11_3_003

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, *20*(5), 28-32. doi: 10.7748/nr2013.05.20.5.28.e327

Dorminey, J. W., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). Financial fraud: A new perspective on an old problem. *The CPA Journal*, *82*(6).

Dull, R. (2014, February). What gets monitored gets detected. *Journal of Accountancy*, *217*(2), 32.

Ebberts, A. M. (2015, Winter). Setting the tone at the top. *Journal of Government Financial Management*, 62-63. Retrieved from https://www.highbeam.com/publications/the-journal-of-government-financial-management-p61847

Elvin, R. (2015, July). Beating the fraudsters. *Chemistry & Industry*, 23. doi: 10.1002/cind.797_5.x

Erickson, S., Lukes, Z., & Weber, M. (2014). Using communication theory to analyze corporate reporting strategies: A study of the health care industry. *Academy of Accounting and Financial Studies Journal, 18*(4), 4-16. doi: 10.1.1.842.5223&rep=rep1&type=pdf

Essays, UK. (2015, March). Theoretical perspective constructivism and naturalistic inquiry psychology essay. Retrieved from https://www.ukessays.com/essays/psychology /theoretical-perspective-constructivism-and-naturalistic-inquiry-psychology-essay.php?cref=1

Ethics Resource Center. (2013). *National Business Ethics Survey of the U.S. Workforce.* Retrieved from https://www.ibe.org.uk/userassets/surveys/nbes2013.pdf

Fountain, L. (2014, August). The fallacies of fraud. *Internal Auditor, 71*(4), 52-57.

Fraud (2018). In *Merriam-Webster's unabridged dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/fraud(

Frazier, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance*, *16*(4), 149-161.

Free, C. (2015). Looking through the fraud triangle: A review and call for new direction. *Meditari Accountancy Review*, *29*(2), 175-196. doi: 10.1108/MEDAR-02-2015-0009

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

Gagliardi, C. (2014). The reality of fraud risk: Five common misconceptions from small business owners. *The CPA Journal*, *84*(4), 11.

Galletta, P. Z. (2015, March). A basic field guide to fraud: Common schemes, relevant cases, and preventative measures. *The CPA Journal*, 54-59.

Gannaway, D. (2013). Fraud prevention tips for business owners and employees. *The CPA Journal*, *83*(6), 12.

Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing intentions of lower-level employees: The effect of reporting channel, bystanders, and wrongdoer power status. *Journal of Business Ethics*, *126*, 85-99. doi: 10.1007/s10551-013-2008-4

Geertz C. (1973). *Toward an interpretive theory of culture: The interpretation of cultures.* New York, NY: Basic Books.

Gerard, J. A., & Weber, C. M. (2016). How agency theory informs a $30 million fraud. *Journal of Finance, Accounting and Management*, *5*(1), 16-47.

Gilmore-Allen, A. (2015, February). Tech fraud and the small business. *Internal Auditor*, 20-21. Retrieved from https://iaonline.theiia.org/2015/tech-fraud-and-the-small-business

Glaser, B. G. (2014). Applying grounded theory. *The Grounded Theory Review*, *13*(1), 46-50.

Glaser, B. G. (86). Strauss. AL (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine.

Glodstein, D. (2009). Ignoring red flags: Perilous consequences for small businesses. *Journal of Forensic Studies in Accounting and Business*, *1*(1), 63-68.

Glodstein, D. (2015). Occupational fraud: Misappropriation of assets by an employee. *Journal of the International Academy for Case Studies*, *21*(6), 125-129.

Grossoehme, D. H. (2014). Research methodology: Overview of qualitative research. *Journal of Health Care Chaplain*, *20*(3), 109-122. doi: 10.1080/08854726.2014.925660

Guercini, S. (2014). New qualitative research methodologies in management. *Management Decision*, *52*(4), 674-662. doi: 10.1108/MD-11-2013-0592

Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting*, *24*, 44-61. doi: 10.1016/j.cpa.2012.01.004

Gunz, S., & Thorne, L. (2015). Introduction to the special issue on tone at the top. *Journal of Business Ethics*, *126*, 1-2. doi: 10.1007/s10551-013-2035-1

Guo, J., Huang, P., Zhang, Y., & Zhou, N. (2016). The effect of employee treatment policies on internal control weaknesses and financial restatements. *The Accounting Review*, *91*(4), 1167-1194. doi: 10.2308/aacr-51269

Hall, J. (2015). Charity begins in the home: Awell-liked employee's fake vendor scheme nets her US$600,000 over three years. *Internal Auditor*, *72*(3), 25-26.

Hall, J. (2016). The anti-fraud moment: Fighting fraud demands more than just awareness. *Internal Auditor*, *73*, 35-37.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review*, *9*(2), 193-206.

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report*, *17*(2), 1-8.

Hayes Jr, A. A. (2013). Inside the huddle: Lessons learned from the $6 million man. *Journal of Government Financial Management*, *62*(4), 54-55.

Helms, G. (2012, April). *Common fraud: A guide to thwarting the top ten*. New York, NY: America Institute of Certified Public Accounts, Inc.

Henry, L. (2016, April). Back to basics: Fraud prevention. *Internal Auditor*, 17-18. Retrieved from https://iaonline.theiia.org/pages/search.aspx?k=back%20to%20basics%3A%20Fraud%20prevention

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2014). Qualitative case study data analysis: An example from practice. *Nurse Researcher, 22*(5), 8-12. doi: 10.7748/nr.22.5.8.e1307

Howard, J. A. (2015, December). A simple control. *Internal Auditor*, 12. Retrieved from https://iaonline.theiia.org/

Hrncir, T., & Metts, S. (2012). Why small businesses fall victim to fraud: Size and trust issues. *Business Studies Journal, 4*(1), 61-71.

Ingram, D. (2018, January). What are the seven internal control procedures in accounting? *Chron.* Retrieved from http://smallbusiness.chron.com/seven-internal-control-procedures-accounting-76070.html

Institute for Fraud Prevention. (2016). *In-process and completed research projects*. Retrieved from www.theifp.org/studies.html

International Organization for Standardization (ISO). (2009). *Standard 31000: Risk Management.* Retrieved from https://www.iso.org/iso-31000-risk-management.html

International Standard on Auditing (ISA). (2017). *Standard 701: Communicating Key Audit Matters in the Independent Auditor's Report.* Retrieved from https://www.ifac .org/publications-resources/international-standard-auditing-isa-701-new -communicating-key-audit-matters

Jahmani, Y., Ansari, M. I., & Dowling, W. (2014). Testing for Internal Control Weaknesses in Accelerated Filers. *Academy of Accounting and Financial Studies Journal, 18*(1), 97.

Jahmani, Y., & Dowling, W. A. (2015). Characteristics of large accelerated filers with internal control weaknesses. *Academy of Accounting and Financial Studies Journal, 19*(2), 129-141.

Jeppesen, J. (2016). From interview to transcript to story: Elucidating the construction of journalistic narrative as qualitative research. *The Qualitative Report*, *21*(9), 1636-1650.

Johnson, E. N., Kuhn Jr, J. R., Apostolou, B. A., & Hassell, J. M. (2013). Auditor perceptions of client narcissism as a fraud attitude risk factor. *Auditing: A Journal of Practice & Theory*, *32*(1), 203-219. doi: 10.2308/ajpt-50329

Kaczynski, D., Salmona, M., & Smith, T. (2014). Qualitative research in finance. *Australian Journal of Management*, *39(*1) 127-135. doi: 10.1177/0312896212469611

Kapp, L., & Heslop, G. (2015, August). A matter of life or death. *Internal Auditor*, 23-24. Retrieved from https://iaonline.theiia.org/2015/a-matter-of-life-and-death

Keller, T. (2012). *Every good endeavor: Connecting your work to God's work*. New York, NY: Penguin Group, Inc.

Kennedy, J. P., & Benson, M. L. (2016). Emotional reactions to employee theft and the managerial dilemmas small business owners face. *Criminal Justice Review*, *41*(3), 257-277. doi: 10.1177/0734016816638899

Kitching, K. A., Pevzner, M., & Stephens, N. M. (2013). Comments by the auditing standards committee of the auditing section of the American Accounting Association on the COSO request for comments on internal control over external financial reporting: Compendium of approaches and examples. *Current Issues in Auditing*, *7*(1), 30-31. doi: 10.2308/cila-50475

Klein, R. (2015, March). How to avoid or minimize fraud exposures. *The CPA Journal*, *85*(3), 6-8.

Kollar, R. J., & Williams, V. C. (2012, April). *Small business fraud awareness, prevention and detection—Hands on consultation with tangible results*. Presented at the Webinar

Conference on Teaching and Learning in Accounting (CTLA) of the American Accounting Association. Retrieved from http://docslide.net/download/link/2012-conference-on-teaching-and-learning-in-accounting-ctla-presented-by

Kramer, B. (2015). Trust, but verify: Fraud in small businesses. *Journal of Small Business and Enterprise Development*, *22*(1), 4-30. doi: 10.1108/JSBED-08-2012-0097

Kroll Advisory Solutions. (2014). *2013-2014 Global Fraud Report*. Retrieved from http://www.kroll.com

Latané, D., & Darley, J. M. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4), 377-383. doi: 10.1037/h0025589

Latham, J. R. (2014). Qualitative sample size: How many participants is enough? *John R. Latham, Ph.D.* Retrieved from www.johnlatham.me/many-participants-enough/

Law, M., & Kusant, R. (2014). An exploration of small business restaurants knowledge and skills to prevent fraud. *Journal of Finance and Accountancy, 17*, 1-15.

Laxman, S., Randies, R., & Nair, A. (2014, February). The fight against fraud: Internal auditors can use COSO components to develop and deliver an effective fraud mitigation program. *Internal Auditor, 71*, 49-53.

Lee, G., & Fargher, N. (2013). Companies' use of whistle-blowing to detect fraud: An examination of corporate whistle-blowing policies. *Journal of Business Ethics*, *114*(2), 283-294. doi: 10.1007/s10551.012-1348-9

Lenz, P. J., & Graycar, A. (2016). Stealing from the boss: Who is looking? *Journal of Financial Crime*, *23*(3), 613-623. doi: 10.1108/JFC-09-2015-0053

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324-327. doi: 10.4103/2249-4863.161306

Levy, H. B. (2015). A fresh look at fraud risk: Guidance for auditors. *The CPA Journal, 85*(10), 6-10.

Levy, H. B. (2016, October). Fighting fraud—and serving Famous Frankfurters—for over a century: The story of old-fashioned controls at Nathan's Famous. *The CPA Journal*, 6-8. Retrieved from https://www.nysscpa.org/news/publications/the-cpa-journal/nathans-famous-fighting-fraud-and-serving-famous-frankfurters-for-over-a-century

Loria, K. (2015, May). Embezzlement? That could never happen in my practice. PTinMOTIONmag.org, 24-33. Retrieved from http://www.apta.org /PTinMotion/2015/5/Embezzlement/

Louwers, T., Ramsay, R. J., Sinason, D. H., Strawser, J. R., & Thibodeau, J. C. (2015). *Auditing & Assurance Services*. New York, NY: McGraw-Hill Education.

Mackevičius, J., & Girūnas, L. (2013). Transformational research of the fraud triangle. *Ekonomika*, *92*(4), 150-163.

Mangala, D., & Kumari, P. (2015). Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce and Accounting Research*, *4*(1), 35-45. doi: 10.21863/jcar/2015.4.1.006

Mann, L. (2013). How to reduce the risk of purchasing fraud. *Healthcare Financial Management, 67*(7), 8-81.

Marais, P., & Ostwalt, P. (2016, May). Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. *KPMG International*, 1-28. Retrieved from https://assets .kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Marquet, C. T. (2017, January). Economic forecasts suggest business opportunities ahead—But persistent risks in 2017 and beyond require vigilance. *Marquet International*. Retrieved from www.marquetinternational.com

McCole, G. (2014, August). All in a dishonest day's work. *Journal of Accountancy*, *218*(2), 20-21.

McMahon, R., Pence, D., Bressler, L., & Bressler, M. S. (2016). New tactics in fighting financial crimes: Moving beyond the fraud triangle. *Journal of Legal, Ethical and Regulatory Issues*, *19*(1), 16-25.

McNally, J. S. (2015). Risk: Leverage it. Control it. Win! *Financial Executive*, *31*(1), 12-19.

McNeal, A. (2016, September). What's your fraud IQ? This month: Employee handbooks and policies. *Journal of Accountancy*, *223*(3), 38-42.

Meyer, H. A. (n.d.). Acts 5:1 commentary. *Meyer's New Testament Commentary*. Retrieved from http://biblehub.com/commentaries/acts/5-1.htm

Mihret, D. G. (2014). National culture and fraud risk: Exploratory evidence. *Journal of Financial Reporting and Accounting*, *12*(2), 161-175. doi: 10.1108/JFRA-10-2012-0049

Miller, B. (2014, June). Employee handbooks: The importance of signed acknowledgements. *HR Daily Advisor*. Retrieved from https://hrdailyadvisor.blr.com/2014/06/17/employee-handbooks-the-importance-of-signed-acknowledgements/

Mittelstaedt, J. D., Harben, G., & Ward, W. A. (2003). How small is too small? Firm size as a barrier to exporting from the United States. *Journal of Small Business Management*, *41*(1), 68-84. doi: 10.1111/1540-627X.00067

Morales, J., Gendron, Y., & Guénin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, *39*(3), 170-194. doi: 10.1016/j.aos.2014.01.006

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212-1222. doi: 10.1177/1049732315588501

Mosalanejad, L., Paransavar, N., Gholami, M., & Abdellahifard, S. (2014). Increasing and decreasing factors of hope in infertile women with failure in infertility treatment: A phenomenology study. *Iranian Journal of Reproductive Medicine, 12*(2), 117-124.

Murphy, P. R., & Free. C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting, 28*(1), 41-56. doi: 10.2308/bria-51083

Neguriţă, O., & Ionescu, I. E. (2016). Risk factors for bank fraud arising as a consequence of misstatements resulting from misappropriation of assets. *Economics, Management, and Financial Markets*, *11*(1), 330-337.

Newman, C. J., & Neier, D. S. (2014, August). Become proactive, not reactive, to anti-fraud and anticorruption programs. *Financial Executive*, *30*(4), 14-17.

Ngwenya, B., & Munyanyi, E. (2015). Assessment of the effectiveness of cash management internal controls in the Zimbabwe Red Cross Society chapter. *International Journal of Research in Commerce & Management*, *6*(3), 12-14.

Nigrini, M. J., & Mueller, N. J. (2014). Lessons from an $8 million fraud. *Journal of Accountancy*, *8*(2), 84-88.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35. doi: 10.1136/eb-2015-102054

Noviyanti, S., & Winata, L. (2015). The role of “tone at the top” and knowledge of fraud on auditors’ professional skeptical behavior. *Contemporary Management Research, 11*(1), 55-74. doi: 10.7903/cmr.12239

Oseifuah, E. K., & Gyekye, A. B. (2013). Internal control in small and microenterprises in the Vhembe District, Limpopo Province, South Africa. *European Scientific Journal*, *9*(4), 241-251.

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, *3*(1), 1-7. doi: 10.15577/jmt.2016.01.1

Patelli, L., & Pedrini, M. (2015). Is tone at the top associated with financial reporting aggressiveness? *Journal of Business Ethics, 126,* 3-19. doi: 10.1007/s10551-013-1994-6

Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance, 16,* 489-497.

Pett, J., Blomster, K., & Wallace, A. (2015, February). A well-oiled machine. *Internal Auditor, 72*, 31-35.

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: An exercise in interviewer self-reflectivity. *Qualitative Research*, *12*(2), 165-185. doi: 10.1177/18791111422107

Phairas, D. (2016). Preventing and recognizing embezzlement. *The Journal of Medical Practice Management*, *31*(4), 209-211.

Playing offense in a high-risk environment. (n.d.) *Crowe Horwath*. 1-12. Retrieved from http://www.crowehorwath.net/uploadedFiles/crowe-horwath-global/IIA/RISK8115_PlayingOffenseWP_lo[1].pdf

Poggenpoel, M., & Myburgh, C. (2003). The researcher as research instrument in educational research: A possible threat to trustworthiness? *Education*, *124*(2), 418-420.

Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society*, *38*, 525-543. doi: 10.1016/j.aos.2012.07.004

Prabowo, H. Y. (2016). Sight beyond sight: Foreseeing corruption in the Indonesian government through behavioral analysis. *Journal of Financial Crime*, *23*(2), 289-316. doi: 10.1108/JFC-12-2014-0053

Prasad, S. (2013, April). Getting to the root cause. *Internal Auditor*, 24-25. Retrieved from https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx

PricewaterhouseCoopers (PwC). (2016). *Global economic crime survey*. London, UK: PwC Publishing. Retrieved from http://www.pwc.com/crimesurvey

Protecting Confidentiality & Anonymity. (2017). Institutional Review Board for Social Behaviorial Sciences, University of Virginia. Retrieved from http://www.irb.vt.edu/pages/confidentiality.htm

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. *Australian Accounting, Business and Finance Journal (AAB&FJ)*, *11*(1), 28-54.

Rice, S. C., Weber, D. P., & Wu, B. (2015). Does SOX 404 have teeth? Consequences of the failure to report existing internal control weaknesses. *The Accounting Review*, *90*(3), 1169-1200. doi: 10.2308/accr-50974

Rittenberg, L. E. (2006, October). Internal control: No small matter. *Internal Auditor*, *63*(5), 47-52.

Roberts, P., Priest, H., & Traynor, M. (2006). Reliability and validity in research. *Nursing Standard*, *20*(44), 41-45. doi: 10.7748/ns2006.07.20.44.41.c6560

Rodgers, W., Söderbom, A., & Guiral, A. (2015). Corporate social responsibility enhanced control systems reducing the likelihood of fraud. *Journal of Business Ethics*, *131*(4), 871-882. doi: 10.1007/s10551-014-2152-5

Rose, M., Sarjoo, P., & Bennett, K. (2015, June). A boost to fraud risk assessments. *Internal Auditor*, 22-23. Retrieved from https://iaonline.theiia.org/2015/a-boost-to-fraud-risk-assessments

Ruankaew, T. (2016). Beyond the fraud triangle. *International Journal of Business Management and Economic Research*, *7*(1), 474-476.

Samuels, J. A., & Pope, K. R. (2014, December). Are organizations hindering employee whistleblowing? *Journal of Accountancy*, *218*(6), 42-44.

Sandhu, N. (2016). Behavioral red flags of fraud—A qualitative assessment. *Journal of Human Values*, *23*(3), 221-237. doi: 10.1177/0971685816650579

Schuchter, A., & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, *39*(3), 176-187. doi: 10.1016/j.accfor.2014.001

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63-75. doi: 10.3233/EFI-2004-22201

Simha, A., & Satyanarayan, S. (2016). Straight from the horse's mouth: Auditors' on fraud-detection and prevention, roles of technology, and white-collars getting splattered with red. *Journal of Accounting and Finance*, *16*(1), 26-44.

Singh, A. S. (2014). Conducting case study research in non-profit organizations. *Qualitative Market Research: An International Journal, 17*(1), 77-84. doi: 10.1108/CJMR-04-2013-0024

Singh, K., Best, P., & Mula, J. (2013). Automating vendor fraud detection in enterprise systems. *Journal of Digital Forensics, Security and Law*, *8*(2), 7-42.

Snelgrove, S. R. (2014). Conducting qualitative longitudinal research using interpretative phenomenological analysis. *Nurse Researcher*, *22*(1), 20-25. doi: 10.7748/nr.22.1.20.e1277

Sorour, M. K., & Howell, K. E. (2013). A grounded theory analysis of corporate governance in Egyptian banking. *Qualitative Research Journal, 13*(3), 289-316. doi: 10.1108/QRJ-03-2013-0017

Southern Development Co. v Silva, 125 U.S. 247 (1888). Retrieved from https://supreme.justia.com/cases/federal/us/125/247/

Spiceland, J. D., Sepe, J. F., Nelson, M. W., & Thomas, W. B. (2016). *Intermediate accounting*. New York, NY: McGraw-Hill Education.

Stake, R. E. (2005). Qualitative case studies. *In* N. K. Denzin and Y. S. Lincoln (Ed.), *The SAGE Handbook of Qualitative Research* (3rd ed.). Thousand Oaks, CA: Sage.

Starman, A. B. (2013, January). The case study as a type of qualitative research. *Journal of Contemporary Educational Studies*, *64*, 28-43.

Steffee, S. (2014, April). Update: Fraud threat spreading. *Internal Auditor,* 13-14. Retrieved from https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx

Stone, R. (2016). Fraud, security, and controls in small businesses: A proposed research agenda. *Journal of Business, 1*(3), 15-21. doi: 10.18533/job.v1i6.44

Stott, J. (1994). Prestige without inconvenience. *Awaiting Epiteleo*. Retrieved from https://kahlich.wordpress.com/tag/john-stott/

Sun, Y. (2016). Internal control weakness disclosure and firm investment. *Journal of Accounting Auditing & Finance*, *31*(2), 277-307. doi: 10.1177/0148558X15598027

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review*, *5*(1), 1-12.

The Accounting Degree Review. (2016). The 10 worst corporate accounting scandals of all times. The Accounting Degree Review.Org. Retrieved from http://www.accounting-degree.org/scandals/

Tonowski, R. (2015). Personnel selection, credit and criminal history and the law. *The Industrial-Organizational Psychologist*, *52*(3), 101-106.

Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley Jr, R. A. (2013). A synthesis of fraud-related research. *Auditing: A Journal of Practice & Theory*, *32*(1), 287-321. doi: 10.2308/ajpt-50360

Trompeter, G. M., Carpenter, T. D., Jones, K. L., & Riley Jr, R. A. (2014). Insights for research and practice: What we learn about fraud from other disciplines. *Accounting Horizons*, *28*(4), 769-804. doi: 10.2308/acch-50816

Tschakert, N., Needles Jr, B., & Holtzblatt, M. (2016). The red flags of fraud: Internal auditors' knowledge of business makes them ideal candidates to detect unethical behaviors. *Internal Auditor*, *75*(5), 60-65.

U.S. Chamber of Commerce Small Business Nation. (2009). Detecting and deterring fraud in small businesses. Retrieved from http://business.uschamber.com

Van der Wal, Z., Graycar, A., & Kelly, K. (2015). See no evil, hear no evil? Assessing corruption risk perceptions and strategies of Victorian public. *Australian Journal of Public Administration*, *75*(1), 3-17. doi: 10.1111//1467-8500-12163

Van Duzer, J. (2010). *Why business matters to God (And what still needs to be fixed)*. Dover Grove, IL: Intervarsity Press.

Van Gent, R. D., Lindquist, T. D., & Smith, G. (2013, September). The six million dollar man: A case study of white-collar crime. *The CPA Journal*, 70-72.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly: Management Information Systems*, *37*(1), 21-54.

Verbruggen, M. (2012). Ananias and Sapphira: A lesson in grace. *Christian Reformed Church*. Retrieved from https://www.crcna.org/resources/church-resources/reading-sermons/ananias-and-sapphira-lesson-grace

Verick, P. (2013, June). Addressing dynamic threats of fraud. *Financial Executive*, *29*(5), 46-50.

Verovska, L. (2014). Internal control system as continuous basis of efficient and stable company development. *Regional Formation and Development Studies*, *3*(8), 240-246.

Verschoor, C. C. (2014). Fraud continues to cause significant losses. *Strategic Finance, 96*(8), 11-85.

Waite, T. (2013). Investigations of wrongdoing: Starting off on the right foot. *Internal Auditor*, *70*(5), 41-44.

Webster, M. D. (2016). Examining philosophy of technology using grounded theory methods. *Qualitative Social Research*, *17*(2), Art. 5.

Wells J. T. (2004). Small business, big losses. *Journal of Accountancy*, *198*(6), 42-47.

Wells, J. T. (2011). *Corporate fraud handbook: Prevention and detection*. Hoboken, NJ: John Wiley & Sons.

Wells, J. T., Kranacher, M. J., & Riley, R. (2011). *Forensic accounting and fraud examination.* Hoboken, NJ: John Wiley & Sons.

Wilkins, A. M., & Haun, A. L. (2014). Reframing the discussion on internal control: Implications of the updated COSO framework for small and entrepreneurial organizations. *The CPA Journal*, *84*(10), 48-51.

Williams, V. T., & Kollar, R. J. (2013). What are the risks? Self-Assessment tool can help small businesses evaluate fraud controls. *Journal of Accountancy*, 215(3), 40-41.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38-42.

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225-231.

Yeasim, S., & Rahman, K. F. (2012). Triangulation research method as the tool of social science research. *BUP Journal*, *1*(1), 154-163.

Yin, R. Y. (2014). *Case study research: Design and methods*. Los Angeles, CA: Sage.

Young, N. (2014, June). How not-for-profits can reduce fraud risk. *Journal of Accountancy*, 44-46. Retrieved from http://www.journalofaccountancy.com/news/2014/jun/fraud-risk-not-for-profits.html

Yusof, M. K., Khair, A. H., & Simon, J. (2015). Fraudulent financial reporting: An application of fraud models to Malaysian public listed companies. *The Macrotheme Review*, *4*(3), 126-145.

Zhang, J., Pany, K., & Reckers, P. M. (2013). Under which conditions are whistleblowing "best practices" best? *Auditing: A Journal of Practice & Theory*, *32*(3), 171-181. doi: 10.2308/ajpt-50451

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2012). Qualitative research tools. *Business research methods* (9th ed.). Mason, OH: South-Western Cengage Learning.

Appendix A: Case Study Interview Questions

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) constructed a model for assessing internal business controls. The five components of the model include factors in the following areas: control environment, risk assessment, control activities, information and communication, and monitoring.

Control Environment

1. Describe the regular activities in which the owner is involved?
2. Does the owner approve new vendors?
3. Does the owner regularly review bank statements and financial records? How often?
4. Does the owner sign checks?
5. How are employees encouraged to report concerns of fraudulent activities to owner?
6. Are financial statements reviewed monthly or quarterly by the owner?
7. Is a cash flow statement prepared by the owner and/or manager?
8. Are customer complaints directed to the owner with no screening?
9. Does the owner approve purchases over a specific dollar amount?

Risk Assessment

1. Are risk assessments conducted regularly?

Control Activities

Human Relations

1. Describe the hiring process.
2. Are employment background checks performed for all employees, including temporary, part-time, and contract workers?

   _____ Past employment

_____ Eligible for rehire

_____ Criminal background

_____ Drug testing

_____ Education and licenses

_____ References

3. Do employees job-share or rotate positions?
4. How are employees' work hours verified?
5. Other than the owner, do any key employees appear to dominate the company?
6. Other than the owner, do any key employees appear to have a close association with vendors?
7. Other than the owner, do any key employees have outside business interests that might conflict with their job duties?
8. Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?
9. Is the hiring process separate from the processing of payroll?
10. Is payroll processed internally?
11. Is the employee payroll list periodically reviewed for duplicate or missing Social Security numbers?

Cash Receipts

1. Describe the cash receipts process.
2. Is a bank lockbox used for processing customer payments?
3. Are deposits made daily and secured prior to depositing in a safe?
4. Are incoming checks restrictively endorsed?

Cash Disbursements

1. Are refunds, voids and discounts evaluated on a routine basis to identify patterns of activity among employees, departments, shifts or merchandise?
2. Are purchasing and receiving functions separate from invoice processing, accounts payable and general ledger functions?

Purchasing and Inventory

1. Describe the purchasing process.
2. Are inventory and supplies secured in a warehouse or place that is restricted?
3. Are inventory or supplies counted on a periodic basis (at least annually)?
4. Is there a competitive bid process?
5. Are purchase orders used for ordering?
6. Are discounts taken for early pay terms?
7. Are blank or unused checks kept secured?

Information and Communication

1. How does the organization educate employees about the importance of ethics and anti-fraud programs?

   ____ Training

   ____ Employee Manual

Monitoring

1. Do you have an external financial statement audit, review or compilation completed?
2. Are surprise audits conducted by management, supervisors, or the owner?
3. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?

4. Does the business have a code of ethics and conflict of interest policy?
5. Is the monthly bank statement received and reviewed by someone other than the person handling the cash and checks?
6. Is a monthly bank reconciliation completed by someone other than the person handling the deposits or with check signing authority?
7. When inventory or supplies are received, is the amount matched with the purchase order? By whom?
8. When vendor invoices are received are they reconciled against receiving reports and purchase orders? By whom?

Adapted from: Williams, V. T., & Kollar, R. J. (2013, February). What are the risks? *Journal of Accountancy*, 40-41. Retrieved from http://www.journalofaccountancy.com/issues/2013/mar/2