Journal of Forensic and Investigative Accounting
Volume 12: Issue 1, January–June 2020

An Exploration of Internal Controls and Their Impact on Employee Fraud in Small Businesses

*Kent Lachney, DBA, CPA**

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.

Purpose and Research Question

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 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?"

Process

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. With the increase in the number of fraud perpetrators, business owners found it necessary to develop a model for assessing and 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.

The researcher developed a 44-question interview (see Appendix A). After the researcher interviewed the owner and/or manager from each business, the researcher then transcribed the interviews and validated the accuracy of the transcripts with the participants. 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.

Background of the Problem

Many small business owners fear bad publicity and cannot afford the time and expense of prosecution; hence, 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* (2018) 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. In fact, most small business owners think they are not at risk for fraud because of the "tone at

* The author serves as Coordinator and Assistant Professor of Accounting at Louisiana State University at Alexandria.

the top" or climate of their organization; they disregard the need for effective internal controls (Gagliardi, 2014, p. 11; Noviyanti and Winata, 2015, p. 55). Further, Law and Kusant (2014) noted the lack of internal controls typically provide situations which lend themselves to fraudulent acts. Small business owners 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 (pressure), 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) 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. There are numerous factors that small business owners can look for to become better aware of potential fraud.

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 and Gyekye, 2013; Jahmani *et al*., 2014; Ngwenya and 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, Milovanovic, and Stancic (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 to monitor organizations to prevent fraudulent activities and promote realistic assurance concerning the achievement of organizational objectives.

Presentation of the Findings

Participant Selection

The researcher selected five participants, based on the study's parameters: small business organizations who were members of the Central Louisiana Regional Chamber of Commerce. According to Mittelstaedt, Harben, and Ward (2003), small businesses are defined as those with fewer than 100 employees. In determining the number of small businesses to study, Creswell's (2013) recommends that no more than four or five case studies be included in a single study. Creswell (2013) explained that this number should provide enough opportunity to identify themes of the cases as well as conduct cross-case analysis.

Following is a brief summary of each of the small businesses studied in this research. Participant 1 is in the lodging industry, which includes a hotel, two restaurants, and a bar/lounge. There is one owner, one general manager over all of the facilities, and 93 employees. The business has a separate human resources department, accounting department, and managers to oversee the housekeeping staff and the culinary team. Each department head reports to the general manager. The participant in this study was the general manager who reports directly to the owner.

Participant 2 is in a physician group, which consists of five physician owners and twelve doctors who practice in eleven locations. The business owners have structured a management group in which the owners act as a board. The organization has 60 employees. The participant in this study was the non-owner CEO. The owners have authorized the CEO and management team to carry out the day-to-day operational activities of the practice.

Participant 3 is in the financial services industry. There are four owners and 19 employees. Their broker/dealer national unit is based in California, but this business is an independent firm. There are two types of employees, licensed and unlicensed. The licensed employees are those individuals who work with the clients' investments. The non-licensed employees are the support staff who work to ensure the proper operation of the business itself. The four owners make all of the day-to-day decisions. The participant was one of the owners.

Participant 4 is in the heating, ventilation, and air conditioning (HVAC) industry. There are three owners and 86 employees. This business provides factory-trained and certified HVAC technicians. The business offers the most complex sheet metal fabrication shop in Louisiana, with the premiere fabrication of steel, stainless, aluminum, and copper products. The participant of this study was the operations manager.

Lastly, Participant 5 is a family-owned business in the office products/office solutions industry that began by selling mainly office supplies and later branched out into office furniture and office equipment. Today, the company also offers janitorial supplies. Consequently, the business offers the full gambit in office solutions, selling to other business organizations. There are two owners and 48 employees. The participant was one of the 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 2018 *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 percent of small business failures were the result of employee fraud. In this study, however, 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. See Appendix B for a summary of each participants' responses.

Control Environment

Each participant's organization was studied to ascertain how the 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 the aspects of the control environment included characteristics of integrity, this element of the model may also 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. All the participants in this study established an ethically strong tone at the top based on an explanation of the organizations' code of ethics policies compared to the findings of the Ethics Resource Center (2013) which reported that 60 percent of misconduct involved someone from the supervisory level up to those individuals holding top management positions. In fact, 24 percent involved senior managers.

Participant 1 (lodging) actively inquired 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.

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. Participant 1 (lodging) 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. Participant 5 stated that the owners selected vendors personally.

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. 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. Participant 1 (lodging) prepared a daily report to the owner which included account balances, available credit limits, pending withdrawals, and pending deposits. Participant 2 (physicians) 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. 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.

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 percent of small businesses implemented hotlines whereas 82 percent 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, Participant 1 (lodging) explained the employee manual also contained the procedure for contacting the employee's supervisor. Participant 2 (physicians) 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."

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.

Participants were asked to describe the risk assessments conducted by their businesses, which varied by industry. For instance, the participants in industries that required government regulations (Participant 2—physicians, Participant 3—financial, and Participant 4—HVAC) were concerned with compliance assessment whereas Participant 5 (office supplies) focused on weekly assessment of competitors. Participant 1 (lodging) 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. Participant 1 (lodging) and Participant 2 (physicians) conducted many compliance risk assessments. Both organizations had a Compliance and Risk Management Department or a specific employee responsible for ensuring compliance and assessing risk. In fact, Participant 2 (physicians) had to follow Health Insurance Portability and Accountability Act (HIPAA), which protects patients' privacy concerning their medical records. They also were 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 regarding technology. The author suggested that organizations need privacy and security policies concerning the use of strong passwords, social media, email, and routine password changes. Participant 3 (financial) assessed risk through its technology by performing an annual technology risk assessment audit on their databases using an external technology group. Participant 2 (physicians) and Participant 4 (HVAC) explained that they had to be compliant with Occupational Safety and Health Administration of the United States Department of Labor (OSHA) regulations. Participant 5 (office supplies) emphasized the risk assessment concerning competition as well as the safety and liability of its delivery drivers.

All 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 Participant 5 (office supplies). 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). 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. All 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.

Participant 1 (lodging) described its detailed hiring process of prospective employees, which included a formal resume as well as at least two interviews and documentation. Telephone reference checks included past employment and a determination as to whether the applicant was eligible for re-hire.

Participant 2 (physicians) 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. 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 (Participant 3), 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 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 family owned office solutions business (Participant 5) often used word of mouth and Facebook to advertise job openings. Since none of these organizations have a formal human resource department, the supervising manager was active in the hiring process. For sales employees in the office solutions business (Participant 5), 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 office supplies 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. 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 the participants in the businesses reported that social security numbers were checked often to ensure there were no ghost employees. All the participants indicated the hiring process was kept separate from the payroll process, except for Participant 5 (office supplies), in which both functions were performed by the owner. The payroll function was conducted internally through a separate department in three businesses, Participant 1 (lodging), Participant 2 (physicians), and Participant 4 (HVAC). Employers also confirmed the number of hours that their employees worked. All the small businesses used a time clock which registered the employees' hours worked. Participant 5 (office supplies) used face recognition software to sign in/sign out whereas the other organizations used either fingerprint ID or an employee number. Participant 1 (lodging) used camera surveillance focused on the clock as the worker clocked in and out. All the organizations stressed the importance of accurately recording hours worked. For example, Participant 1 (lodging) 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 percent 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 potentially fraudulent activities. 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. Since these are small businesses, the owners and/or managers would be aware if someone refused to take a vacation. 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.

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. Moreover, Klein (2015) pointed out that employees should have limited authority over any transaction or accounting function. In fact, Participant 2 (physician) indicated the process was quite detailed. For example, one employee oversaw Accounts Payable. Then, both the accounting manager and CEO approved and initialed each check requested. Finally, one of the owners signed the check. Participant 3 (financial) 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 the office supplies business (Participant 5), only one signature was used on checks for large amounts since the check signor was an owner. Otherwise, two signatures were required. In all of the businesses, employees were trained for more than one job, so they could replace another person temporarily.

Cash receipts and disbursements. Dull (2014) recommended that blank checks, cash and customer checks received should be kept secure until they are processed. Since Participant 1 (lodging) received a significant amount of cash daily, there was a multiple-step process for receiving and verifying cash. In addition, this participant installed security cameras over all 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. All 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. Participant 2 (physicians) required authorization from two employees if the amount was over $100. In addition, one of the owners signed refund checks. In another business, (Participant 3, financial) the national broker/dealer provided cash disbursements to the clients rather than the local business. Participant 4 (HVAC) and Participant 5 (office supplies) explained that when merchandise was returned, the businesses followed a three-part process: the goods are returned, 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. Stone (2016) reported that cash skimming and larceny were reported twice as often in small businesses. Of the small businesses studied, only Participant 3 (financial) 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 the participants reported strictly professional relationships with vendors who were approved by an owner. However, since Participant 2 (physicians) 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.

Information and Communication

Business organizations must provide and encourage effective communication with their employees. 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. 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. According to McNeal (2016), a written personnel manual should include the organization’s mission statement, core values, and all company policies and practices. 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. 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. Participant 1 (lodging) 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. 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. Participant 2 (physicians) 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. Participant 4 (HVAC) also provided a basic personnel manual; however, the manual was not as detailed since it did not include all the items recommended for a good personnel manual, such as the topics listed in the manuals provided by the two participants mentioned previously. The office supplies business (Participant 5) 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 explanation emphasized the importance of drivers maintaining their professionalism because the owner considered the company truck as the greatest advertisement for the business.

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 another 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.

Participant 3 (financial) explained that their business industry requires extensive ethics and anti-fraud training. Although this training was only required only for licensed employees, this organization also provided the training to non-licensed employees. Participant 1 (lodging), Participant 2 (physicians), and Participant 4 (HVAC) offered training that would improve job performance. Participant 5 (office supplies) took a different approach. The business did not have any type of training program. 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.

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. 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 can minimize opportunity using 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. 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, an ongoing and/or separate evaluation 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. The ACFE *Report to the Nations* (2016) indicated that 40 percent of the fraud tips received were made from nonemployees, such as customers and suppliers. The participant in the lodging business (Participant 1) created an anti-fraud climate by authorizing supervisors, service team, and front desk staff the permission to immediately handle customer concerns. Participant 2 (physicians) indicated that patients and vendor complaints were handled by its human resource/marketing department. Participant 3 (financial) indicated that any complaint that was reported to the owner had to be reported to and handled by its broker/dealer as per financial industry standards. Participant 4 (HVAC) 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. Participant 5 (office supplies owner) 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.

Participant 2 (physicians) 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. Participant 3 (financial) explained 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. Participant 1 (lodging) 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. Participant 4 (HVAC) and Participant 5 (office supplies) 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). Participant 2 (physicians), Participant 4 (HVAC), and Participant 5 (office supplies) 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 e-mail, 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. Participant 1 (lodging) was the only business that 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. Participant 1 (lodging) explained that extensive changes had been made in the areas of the personnel manual and employee training. Participant 2 (physicians) explained that after reviewing purchasing procedures, it became obvious to the owners that it became complicated when satellite offices ordered their own supplies and inventory. Consequently, now all purchases must be made at the main office. The financial business (Participant 3) 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. Participant 4 (HVAC) 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. Participant 5 (office supplies) adapted many changes in its product mix over the years to become a comprehensive office solutions company. However, the participant made few changes regarding 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.

Reflections and Recommendations for Further Study

After reflecting on the effectiveness of the questionnaire, the researcher recommends that revisions should be made in future studies. 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, questions on the survey should address each of the 17 principles within the five components of the COSO model (See Appendix C). In addition, questions should require open ended responses.

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 division might indicate a greater need for education in appropriate internal controls and in preventing and detecting employee fraud in younger organizations. Second, I recommend 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.

Benjamin Franklin's (1735) axiom stated "An ounce of prevention is worth a pound of cure" can be appropriately applied to 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

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

Beach, C. S., and 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.

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

Brody, R. G., Melendy, S. R., and 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., and 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

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

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

Cotton, D. L., Johnigan, S., and 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 and research design: Choosing among five approaches*. Thousand Oaks, CA: Sage.

Dimitrijevic, D., Milovanovic, N., and 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

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

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

Ettish, A. A., El-Gazzar, S. M., and Jacob, R. A. (2017). Integrating internal control frameworks for effective corporate information technology governance. *JISTEM - Journal of Information Systems and Technology Management*, *14*(3). doi: 10.4301/s1807-17752017000300004

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., and 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.

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

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.

Gullkvist, B., and 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

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

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%20 Fraud%20prevention

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

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

Kapp, L., and 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

Kitching, K. A., Pevzner, M., and 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.

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

Law, M., and 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., and 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.

Lenz, P. J., and 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

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

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.

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

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., and 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

Murphy, P. R., and 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., and 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.

Ngwenya, B., and 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 and Management, 6*(3), 12–14.

Noviyanti, S., and 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., and 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.

Patelli, L., and 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

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

Rae, K., Sands, J., and 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 (AABandFJ), 11*(1), 28–54.

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

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

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.

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

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

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

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.

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

Wilkins, A. M., and 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., and 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., and Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38–42.

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

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

Are risk assessments conducted regularly?

Control Activities

Human Relations

Describe the hiring process.

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

Do employees job-share, rotate positions, or have required vacations?

How are employees' work hours verified?

Other than the owner, do any key employees appear to dominate the company?

Other than the owner, do any key employees appear to have a close association with vendors?

Other than the owner, do any key employees have outside business interests that might conflict with their job duties?

Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?

Is the hiring process separate from the processing of payroll?

Is payroll processed internally?

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., and Kollar, R. J. (2013, February). What are the risks? *Journal of Accountancy*, 40–41. Retrieved from http://www.journalofaccountancy.com/issues/2013/mar/2

Appendix B: Summary of Participant Answers to Interview Questions

COSO Element	Question	Participant 1 Lodging	Participant 2 Physicians	Participant 3 Financial	Participant 4 HVAC	Participant 5 Office Supplies
Control Environment	1. Describe the regular activities in which the owner is involved?	Daily review; Profit and Loss statements	Weekly review operational issues; 1–2 times annually to review strategic plan; monthly-financial statements and compare to budget	Final authority; oversight of compliance and expenses	All aspects	All aspects personalities/ HR; A/R-A/P
	2. Does the owner approve new vendors?	No	No	Yes	Yes	Yes
	3. Does the owner regularly review bank statements and financial records? How often?	Yes; third party audit; uses corporate address; owner receives and then sends to accountant; participant reviews daily and compiles reconciliation from point of sale and property management and A/R-A/P; monthly reviews bank statements and reconciles	Monthly; prepare management report, including transactions and PandL; Owners do NOT review actual bank statements, just reviews reconciliation	Yes; monthly	Yes; weekly	Yes; daily
	4. Does the owner sign checks?	Yes	Yes	Yes, if over a set amount	Yes, weekly, but daily as needed	Yes
	5. How are employees encouraged to report concerns of fraudulent activities to owner?	Have detailed procedures manual; 24 hour surveillance of property	Compliance officer and training according to federal law; exit interviews; quarterly interviews with that	One owner designated and remains anonymous	Yes	Make sure they know that this is their company too; pride; ownership

			specific question			
	6. Are financial statements reviewed monthly or quarterly by the owner?	Daily; “Very, very involved; holds bank balances in his head for all businesses”	Monthly	Monthly	Monthly	Monthly
	7. Is a cash flow statement prepared by the owner and/or manager?	Participant but overseen by CPA by remote login	Part of financial management report	No; outside accountant provides monthly report	Yes; weekly	CPA works with participant on cash flow statement
	8. Are customer complaints directed to the owner with no screening?	Supervisors handled right away; very seldom to owner	Can be but usually handled by HR and marketing department	Yes, but because of industry standards it would have to be reported to and handled by broker/ dealer level; owners handle interoffice/ internal concerns	No; screened and directed to assigned owner	Yes
	9. Does the owner approve purchases over a specific dollar amount?	Purchases made by several people; if fixed asset, participant would get 3 bids and get owner's approval over $2,000	Capital projects; over $10,000	Yes	Yes	Yes
Risk Assessment	1. Are risk assessments conducted regularly?	Insurance, interest rates, lines of credit (daily); credit cards; mortgage; workers' comp (monthly); self-insured	Government involved-tax proposal; legal issues, doctors-malpractice; HR; HIPA; OSHA, travel; compliance and risk management department	Internal compliance person; HR; licensure; continuing education	Yes; daily	Competition (weekly); drivers-installed new program; safety
Control Activities	1. Describe the hiring process.	Formal resume; documentation; two	HR dept. and HR manager; applications, no resumes;	2 prongs (licensed and unlicensed employees);	Application; interview by department heads;	Sales manager hires salespeople; uses websites for

Human Relations	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	interviews; checks past employment, criminal background since zero tolerance for drugs, alcohol, bullying, cyberbullying; drug testing; education/ licenses; references; motor vehicle	interview; HR screens, then manager interviews (at least 3 interviews); readiness assessment through the Office of Workforce Development; references; drug screening; if person is in financial, then credit analysis	licensed-owners make decision, then office manager does background, fingerprinting, references drug test; if unlicensed-office manager hires; uses word of mouth advertising	operations manager approves	advertising; sales coach also interviews; personality test; advertise by Facebook for other employees and owner hires
	3. Do employees job-share, rotate positions, or have required vacations?	No	No	No	No	No
	4. How are employees' work hours verified?	Fingerprint time clock	Time clock	Time clock	Time clock	Face recognition time clock
	5. Other than the owner, do any key employees appear to dominate the company?	No	No	No	No	No
	6. Other than the owner, do any key employees appear to have a close association with vendors?	No	No	No	No	No
	7. Other than the owner, do any key employees have outside business interests that might conflict with their job duties?	No	No	No	No	No

	8. Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?	No	No	No	No	No
	9. Is the hiring process separate from the processing of payroll?	Yes	Yes	Yes	Yes	Yes
	10. Is payroll processed internally?	Yes	Yes	No	Yes	No
	11. Is the employee payroll list periodically reviewed for duplicate or missing Social Security numbers?	Yes	Yes	Yes	Yes	Yes
Cash Receipts	1. Describe the cash receipts process.	Handle a lot of cash; received then balanced by night auditor; morning audits again, deposited, reconciled by CPA	Patient brings a form to checkout; cashier puts in envelope; safe; next morning two people count and deposit	Can't hold checks overnight; electronically deposited; copied and uploaded to broker/dealer; after deposit, verify amount	Cash received, put in envelope; receipted to A/R; envelope and receipt deposited and credited to customer	Checks are deposited daily; deposit and checks matched; confirmed deposit when reconciling bank statement
	2. Is a bank lockbox used for processing customer payments?	Yes; used as a cash register which cannot be opened by key, must have physical transaction to open; camera above all cash drawers	No	No	No	No
	3. Are deposits made daily and secured prior to depositing in a safe?	Yes	Yes	No	Yes	Yes
	4. Are incoming checks	Yes	Yes	Yes	Yes	Yes

	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?	Yes	Yes	Yes	Yes	Yes
	2. Are purchasing and receiving functions separate from invoice processing, accounts payable and general ledger functions?	Yes	Yes	Yes	Yes	Yes

Purchasing and Inventory	1. Describe the purchasing process.	Food service manager and hospitality manager submit purchase order	Senior eye technician goes through vendor items; makes order; inventoried; confirm on patient statement	Office manager/staff keep inventory of supplies; office manager orders as needed	Vendor prepares quote, purchase order prepared; received; assigned to job	Owner purchases
	2. Are inventory and supplies secured in a warehouse or place that is restricted?	Yes	Yes	Accounting firm does inventory for depreciation	Yes	Yes
	3. Are inventory or supplies counted on a periodic basis (at least annually)?	Yes; full inventory monthly; quantities assigned to each housekeeper; supplies inventoried weekly	Yes; monthly with barcodes	No	Yes	Yes
	4. Is there a competitive bid process?	Yes	Yes	Yes	Yes	Yes

	5. Are purchase orders used for ordering?	Yes	Yes	Yes	Yes	Yes
	6. Are discounts taken for early pay terms?	Yes	Yes	Yes	Yes	Yes
	7. Are blank or unused checks kept secured?	Yes	Yes	Yes	Yes	Yes
Information and Communication	1. How does the organization educate employees about the importance of ethics and anti-fraud programs? *Training *Employee Manual	Employee manual; staff meetings	Orientation process; mandatory office general compliance training; employee manual; staff meetings	Employee manual; mandatory confidentiality agreements; licensed employees must do annual ethics/ant-fraud training; confidentiality training	Training; employee manual	Set example; no training; no employee manual
Monitoring	1. Do you have an external financial statement audit, review or compilation completed?	Yes	Yes	Yes	Yes	Yes
	2. Are surprise audits conducted by management, supervisors, or the owner?	Yes	Yes	Yes	Yes	Yes
	3. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?	No	No	No	No	No
	4. Does the business have a code of ethics and conflict of interest policy?	Yes	Yes	Yes	Yes	No
	5. Is the monthly bank	Yes	Yes	Yes	Yes	Yes

	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?	Yes	Yes	Yes	Yes	Yes
	7. When inventory or supplies are received, is the amount matched with the purchase order? By whom?	Yes	Yes	Yes	Yes	Yes
	8. When vendor invoices are received, are they reconciled against receiving reports and purchase orders? By whom?	Yes	Yes	Yes	Yes	Yes

Appendix C: COSO Components and Principles

Component 1: Control Environment

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Component 2: Risk Assessment

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Component 3: Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Component 4: Information and Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Component 5: Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Source: Ettish, A. A., El-Gazzar, S. M., and Jacob, R. A. (2017). Integrating internal control frameworks for effective corporate information technology governance. *JISTEM - Journal of Information Systems and Technology Management*, *14*(3). doi: 10.4301/s1807-17752017000300004