2016

Best Practices for Internal Controls to Prevent Occupational Fraud in Small Businesses?

Stephanie Shao
Portland State University

BEST PRACTICES FOR INTERNAL CONTROLS TO PREVENT OCCUPATIONAL FRAUD IN SMALL BUSINESSES

by
Stephanie Shao

An undergraduate honors thesis submitted in partial fulfillment of the

requirements for the degree of

Bachelor of Science

in

University Honors

and

Accounting

Thesis Adviser

Dr. Melissa M. Appleyard

Portland State University
2016

TABLE OF CONTENTS

INTRODUCTION

OCCUPATIONAL FRAUD

Most fraud cases in the news are the high profile financial statement fraud cases where perpetrators have misrepresented the assets and value of a company and have thereby cheated stakeholders of millions of dollars. The names Bernie Madoff, HealthSouth, and WorldCom come to mind. However, a much more insidious type of fraud is afoot in America's business community: small business fraud.

Fraud is a growing issue that organizations face. Occupational fraud refers to the white collar crimes that occur within businesses and is defined by the Association of Certified Fraud Examiners (ACFE) as, "…the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE, 2015, p. 1.201).

In the 2016 *Report to the Nations*, the ACFE estimated that organizations typically lose 5% of revenues each year to fraud (ACFE, 2016). This is a large proportion of revenues that most businesses cannot afford to lose. The ACFE also found that the total losses in their case studies was reported to be $6.3 billion, with an average loss of $2.7 million per case (ACFE, 2016).

The focus of this thesis is on the most common form of occupational fraud: asset misappropriation. This form of fraud makes up 83% of all cases reported to the ACFE (ACFE, 2016). While asset misappropriation has the smallest median loss compared to financial statement fraud or corruption, the ACFE still found that the median loss per case is $125,000 for all organizations, whether for-profit or not-for-profit. This may not present too large of a burden for larger organizations, however this median loss would affect smaller businesses quite differently.

SMALL BUSINESSES

Small businesses are defined by the United States Small Business Administration as organizations with less than $5 million in revenue and less than 500 employees (U.S. Small Business Administration, 2016). In contrast, the ACFE defines small business as organizations with fewer than 100 employees.

As this research will be focusing specifically on occupational fraud occurring in small businesses, the ACFE's definition of small business will be

followed. This will allow the findings from the research to be better tailored to the capstone client for whom this thesis will provide recommendations.

CHARACTERISTICS AFFECTING FRAUD RISK

There are several characteristics prevalent within small businesses that make them particularly vulnerable to occupational fraud.

Having a culture that is too trusting can put the business at risk for fraud, when the business owner trusts all of their employees and does not adopt monitoring procedures (Wells, 2003). However according to the ACFE, 30% of incidents of fraud in their 2016 data were committed by employees or non-owners. Perpetrators tend to be those employed by the organization, because they know the weaknesses and how to exploit them best. Wells (2003) recommends to trust but verify, when it comes to hiring practices. Murphy and Dacin (2011) also found that the organizational climate has a large influence on whether fraud is committed or not in an organization.

Another aspect of the trusting culture is the belief that the business is too small to be targeted (Gagliardi, 2014). This is not true, because smaller organizations face the same vulnerability as their larger counterparts. However, because smaller businesses usually have less liquidity they are often experience a greater effect. Smaller businesses also have easier access to physical assets, which can put a business greatly at risk (Grollman & Colby, 1978).

In addition, because smaller businesses have fewer employees, many internal controls are more difficult to implement (Carland et al., 2001; Johnson & Rudesill, 2001; Wells, 2003; Kapp & Heslop, 2011; Laufer, 2011; Gagliardi, 2014). This means that internal controls, which are important for organizations of any size, tend to be weaker within small private businesses. Because each employee tends to wear more hats, the implementation of internal controls systems is affected greatly. A good example of this is the difficulty in implementing segregation of duties, which will be discussed more within the literature review.

Staffing constraints also usually mean that small businesses lack awareness of fraud on the part of business owners and thus also lack fraud training for employees (Grollman & Colby, 1978; Laufer, 2011). Because the talents of most owners do not lie within finance or accounting realms, there is a lack of understanding of the relationship between internal controls and fraud. This in turn means that there is usually less management oversight, which is extremely important in preventing and detecting occupational fraud (Grollman & Colby, 1978).

SMALL BUSINESS FRAUD

Two-thirds of all fraud cases reported to the ACFE either came from for profit companies (ACFE, 2016). However, the risk characteristics mentioned previously make small businesses much more vulnerable to fraud than larger organizations.

The ACFE (2016) reports that 30% of fraud victims within their study were small businesses with less than 100 employees. While the median loss per fraud case is the same at $150,000 for for-profit organizations of any size, the frequency of fraud at small businesses is much higher than at large businesses (ACFE, 2016).

Though $150,000 may not seem like a big loss for a Fortune 500 company, this amount can be extremely damaging to a small business. A study by Carland et al. (2001) attributed the majority of small businesses failures to occupational fraud. The same study also found that the main modes of failure attributable to occupational fraud were the undercapitalization and lack of strong record keeping at small businesses. Undercapitalization can shut down a small business, because small businesses generally have large amounts of debt and not very much cash. Losing funds to fraud during in this situation means that small businesses either have to close or borrow large sums of money to continue business operations.

In addition, a study by Johnson and Rudesill (2001) estimated that 30% of small businesses fail due to fraud. Hodgetts and Kuratko (1998) found that 35% of collapses could be directly attributed to record keeping issues promulgated by fraud. Combined with the estimation that small businesses experience fraud at 100 times the rate at large businesses, the survival rate of small businesses is under threat by fraud (Wells, 2003). This is further compounded for newly established small businesses, as these businesses tend to have negative cash flows and profits in the first few years of existence.

However, the true number of fraud cases in small businesses is difficult to estimate as small business proprietors are unlikely to detect fraud and are even less likely to report a crime (Finerman, 1995; Carland et al., 2001). Doost (1990) estimated that more than 75% of white collar crime is not reported. This number of unreported crimes is also known as the dark number, as termed by Taylor (2002). Taylor (2002) found that in Australia, only 20% of employee fraud is reported. In the United States, nine out of ten burglaries were reported to the authorities, but employee theft was not reported (Taylor, 2002). This means that the current estimates are grossly underestimated, because the dark number of unreported fraud is large.

What these statistics indicate is that fraud should especially be of concern to small business owners, especially those that do not possess extensive experience running a business. This is the case of my capstone client; from here on out known as the 'client.' As my client is a new business owner without previous experience, the business is at high risk for occupational fraud.

While internal controls have been shown to help minimize the occurrence of fraud, setting an internal controls system up can be difficult in many ways. Thus, it is would be extremely beneficial for small business owners such as my client to receive a recommendation report on how best to prevent fraud in their new businesses through implementable internal controls. As part of this thesis, a literature review will be conducted and findings will be formulated to provide best practice recommendations to the client.

LITERATURE REVIEW

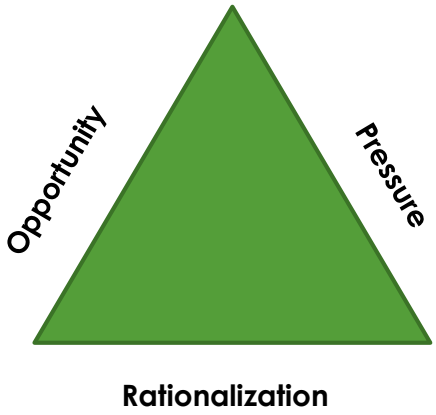
MODELS OF FRAUD THEORY

Before creating an effective fraud internal controls system, the components of fraud must first be understood. Why do perpetrators commit fraud? What are the theories behind what draws individuals to commit white collar crime?

TRADITIONAL FRAUD THEORY

The traditional fraud triangle was established by Cressey (1953), the first researcher to delve into the criminology behind fraud. Cressey's classic fraud theory, first appeared within his fraud textbook in 1953 entitled, *Other People's Money*. His model is based on three components, which create the fraud triangle.

Figure 1 Cressey's Classic Fraud Triangle



The three components are opportunity, pressure, and rationalization. Opportunity refers to whether or not a person has opportunities to commit fraud. Opportunities could exist if there are not adequate internal controls to prevent fraud. This is the aspect that can be most easily controlled. Pressure refers to the personal motivation behind committing fraud. This is more difficult to influence as it is far more complex, and the pressure a person feels can go beyond simple financial pressure. Finally, there is rationalization, which describes the reason(s) a person uses to explain away inhibitions to commit fraud.

Cressey believes that for fraud to occur, a situation must have all three components. This traditional model is heavily supported by audit regulators such as the American Institute of Certified Public Accounts (AICPA)'s Auditing Standards Board (ASB) and the International Audit and Assurance Standards Board (IAASB). The ASB and IAASB showed support for Cressey's model through recent audit standards published in 2002 and 2009. The Committee of Sponsoring Organization's Treadway Commission (COSO) also issued a report in 1987 supporting Cressey's model (COSO, 1987). Thus audit regulators around the world support Cressey's original fraud theory model.

MODERN FRAUD THEORY

There is significant debate within the accounting community regarding the different components of the fraud triangle though. Some believe that the theory is outdated and needs to be adjusted to better suit the modern business environment.

The most heavily debated component is the pressure component. Lister (2007) introduces the idea that while pressures may be present in a person's life, it does not actually mean the person will perpetrate fraud. He views pressure as the motive behind what drives a person to commit fraud and categorizes it into three different types: personal or lifestyle pressure; employment pressure; and external pressure. Personal pressure consists of personal greed. Employment pressure exists when compensation structures are based on commissions or certain targets. External pressure exists when there are market or analyst expectations that must be met. Lister believes that for fraud to be perpetrated opportunities have to exist for these pressures to be released.

Murdock (2008) further develops the idea of multi-faceted pressures by categorizing pressure into financial, non-financial, political and social pressures. Non-financial pressure is related to gambling addictions or substance abuse. Political and social pressures are related to lifestyle and maintaining a reputation

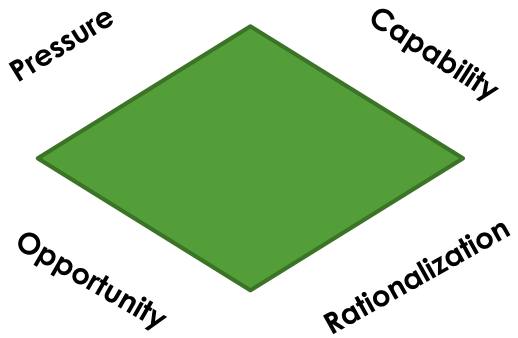
or status. Murdock believes that this view better illustrates that the motivation to commit fraud can stem from different areas of a person's life.

Another view is that fraud is committed when there is both an opportunity and the ability to conceal the fraud (Vona, 2008). This view is also espoused by Albrecht et al. (2008), who propose splitting pressure into financial and non-financial. However, they argue that as long as an individual believes that committing fraud will result in detection and punishment, even strong pressure will not persuade the individual to commit fraud. The ACFE (2016) report supports this concept with the finding that 94.5% of people committing fraud take great efforts to hide evidence of their fraud as they fear being caught. This view plays into Rose et al.'s (2015) research that linked the efficacy of internal controls to lowered fraud frequency as the fear of being caught increased when there were strong internal controls.

Since 1953, additional models of fraud have also appeared. One of these newer fraud models proposes a fourth leg that would turn the triangle into a fraud diamond (Wolfe & Hermanson, 2004). This fourth leg is described by Wolfe and Hermanson (2004) as a capability aspect that is the "personal traits and abilities that play a major role in whether fraud may actually occur even with the presence of the other elements." There are five aspects to this new component:

1. High positional authority allowing for the creation or exploitation of opportunities for fraud that others do not have
2. Necessary intelligence and understanding of internal controls to exploit their weaknesses
3. Confidence and narcissism that they will not get caught
4. Persuasive personality to convince others to follow
5. Ability to lie effectively and consistently
6. Ability to deal well with stress.

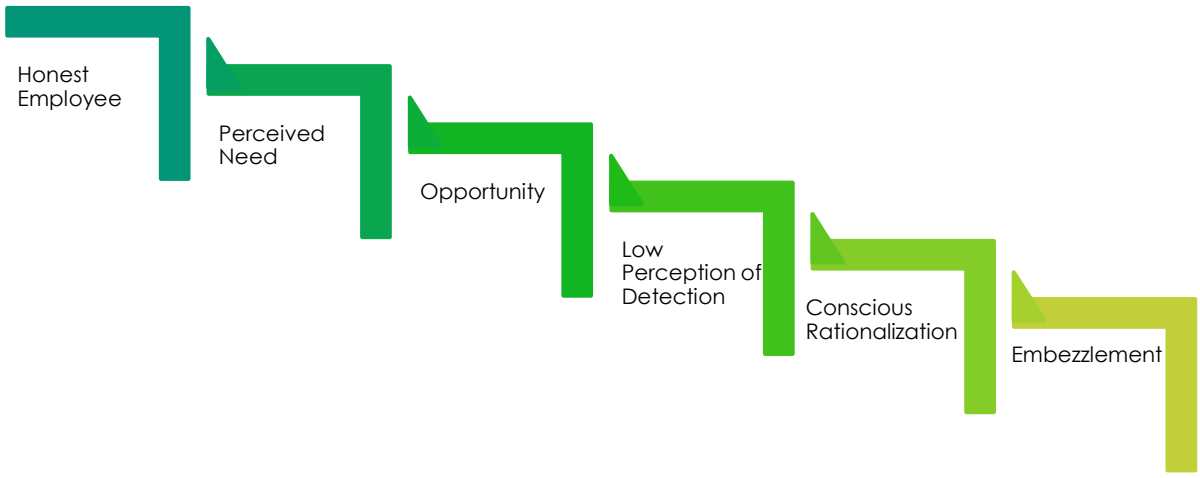
Figure 2 Wolfe and Hermanson's Fraud Diamond Model



Wolfe and Hermanson's (2004) model is based on the idea that an individual may perceive pressure to commit fraud, but it takes an opportunity for fraud to occur. In addition, the individual must be able to rationalize why they are committing fraud. Finally, without the capability component present, they believe that the individual would not be able to commit fraud.

The fraud model that inspired the fraud diamond and other theories is the slippery slope of fraud model presented by Carland et al. (2001). This model illustrates how an honest employee could end up embezzling funds from their workplace.

Figure 3 The Slippery Slope of Fraud



While there are many models of fraud, they all stress that similar components must be present for an individual to commit fraud. A strong understanding of what drives perpetrators to misappropriate assets will allow a stronger internal controls system to be designed and implemented.

PROFILE OF A FRAUD PERPETRATOR

The profile of a fraud perpetrator matches with the capability aspect of the slippery slope fraud model. The ACFE Fraud Examiners Manual (2015) provides profiles of criminals based on past defendants who were charged with fraud. The ACFE (2015) describes the average white collar criminal as someone whose occupational state is professional or at least semi-professional. They work in a career that allows them to utilize specialized skills.

The criminal profile indicates white males, of middle class and moderate social status, with more education than the general population. They are more likely to have a high school diploma or college degree than the average American (ACFE, 2015). The capability aspect proposed by Wolfe and Hermanson (2004) indicates an individual who is intelligent enough to understand where the weaknesses are within an organization to exploit them. This is consistent with the educational level and that the criminals tend to have occupations that are professional or semi-professional. The profile also indicates that it is often very important for the criminal to maintain a certain status or level of respectability. This relates to the perceived personal or lifestyle pressure that leads an individual to commit fraud.

There are two distinct fraudster types: one who is a common fraudster; and one who is a predator (Kapp & Heslop, 2011; Dominey et al., 2012). The common fraudster tends to follow the profile that the ACFE (2015) identifies and is usually tempted by a mix of perceived pressure and opportunity. This individual is easier to catch than the predator. The predator is far more deliberate and may start working at a small business purposefully while planning to commit fraud. This type of individual is more organized, has better understanding of the way the business operates, and is better at concealing any evidence of fraud. This predator type ranks far higher in the capability component of the fraud diamond model.

For the predator type of perpetrator, there are certain internal controls that are recommended to prevent them from committing fraud. While internal controls during hiring is important and will be discussed below, it is important to note that 87% of fraud perpetrators have never been charged with a crime and 84% have never been previously punished or terminated for a fraud related offense (Gagliardi, 2014). This is because most fraud perpetrators are actually model employees. They almost never take vacation time, are willing to come in early or stay late, and they are usually very trusted by the business owner (Kapp & Heslop, 2011).

COMMON FRAUD SCHEMES

As mentioned in the introduction, asset misappropriation, the theft of an entity's assets, is by far the most common type of occupational fraud. It makes up 83% of all cases reported to the ACFE (ACFE, 2016). There are three major categories of asset misappropriation schemes: cash receipts; fraudulent disbursements; and theft of inventory or non-cash assets (ACFE, 2015).

This thesis focuses primarily on misappropriations of the cash asset, as it tends to be the most vulnerable asset of a business. Cash is vulnerable to theft mainly because it is the most liquid asset and because it can be hard to track. In fact, Wells (2003) found that 90% of occupational fraud cases involved cash. This is why the first two major categories of asset misappropriations schemes deal with cash. While theft of inventory and non-cash assets does occur, it is less common as it is more difficult to convert inventory into currency (Wells, 2003).

Cash also tends to be the focus of most accounting entries, as it is recorded any time there are cash receipts and disbursements, and these are the two most vulnerable opportunity points for fraud to occur. Misappropriation of cash can occur on-book or off-book, either before cash is recorded or after.

As mentioned earlier the first major category of asset misappropriations occurs at cash receipts. The two schemes that fall into this category are skimming and larceny. Skimming is defined by the ACFE as "removal of cash from a victim entity prior to its entry in an accounting system" (ACFE, 2015, p. 1.301). This means that skimming occurs off-book, before an accounting entry records the receipt of cash. This is listed in the Fraud Examiners Manual as one of the most common fraud schemes (ACFE, 2015). It is also one of the most common fraud schemes for organizations with less than 100 employees (ACFE, 2016). Skimming is an especially large threat to newly established small businesses, because the business owner's attention is rarely on preventing employees from skimming funds.

The second type of cash receipts fraud is larceny. Larceny is similar to skimming but the main difference is that it occurs after the cash has been recorded. This generally occurs as theft of cash from registers, altering cash counts, or manipulating sales records.

The other common fraud schemes in small businesses include billing schemes and check tampering (ACFE, 2016; Daigle et al., 2009). Billing schemes are where invoices are submitted for fictitious goods or services, which the organization then pays. Check tampering can occur when a perpetrator misuses and alters a business's checks for fraudulent purposes.

While there are many more types of fraud schemes, the focus of this thesis is on skimming and larceny, which have been shown to be twice as likely to occur in smaller organizations than larger ones (ACFE, 2016).

SUMMARY OF FINDINGS

PREVENTING FRAUD THROUGH INTERNAL CONTROLS

Researchers agree that the primary method to prevent occupational fraud is to rely on internal controls systems (Kapp and Heslop, 2011; Gagliardi, 2014; Laufer, 2011; Snyder et al., 1989). However, there is much disagreement which controls work best, what the efficacy of internal controls systems are, and how best to improve them.

The Federal Accounting Standards Board's (FASB) Statement on Auditing Standards no. 1 defines the objectives of internal controls as to provide reasonable assurance that: (1) transactions executed are authorized; (2) recorded transactions are necessary for preparation of financial statements or to maintain asset accountability; (3) access to assets is limited to only those authorized; and (4) accountability for assets is intermittently compared to existing assets. FASB believes that only when these objectives are met, can internal controls help in fraud prevention. Internal controls systems also help businesses run effective and efficient operations and stay compliant with regulations (Laufer, 2011). Grollman and Colby (1978) cite strong internal controls as a method to increase productivity in firms, because controls can help prevent unintentional errors and minimize waste as well as discourage fraud (1978).

There are two types of internal controls: preventive and detective controls. Preventive controls are those that can help prevent fraud from occurring. A good example of a preventive control is requiring authorizing signatures from management on expense reimbursement forms. This prevents expenses from being reimbursed that were not reviewed by management. Detective controls are those that help uncover a fraud scheme. They are generally less popular than preventive controls since when they are found to be working, fraud has already occurred. A good example of a detective fraud is when a manager at a store reconciles the starting cash balance with sales and the ending cash balance. This can help the manager uncover any missing cash immediately.

These two types of internal controls also apply to two different stages within the fraud cycle (Ramamoorti and Dupree, 2010). There is the proactive stage, which utilizes preventive controls to minimize fraud opportunities. There is also the reactive stage, which relies on detective controls to discover the fraud after it has already occurred.

Once the fraud has occurred or a control deficiency has been discovered, compensating controls may be applied to reduce an adverse

financial reporting effect (Gramling et al., 2010b). Compensating controls can be preventive or detective controls that are applied to a business when there are control deficiencies and work as a bandage.

If for example, the previous preventive control of requiring management review of expense reimbursements before they were processed did not work because management never took the time to authorize reimbursements day to day, then a strong compensating control would be requiring receipts to be attached to the reimbursement form. This way the person in charge of reimbursements can verify that the expense is valid and exists.

As seen in this example, compensating controls are generally used when an actual control is too expensive or time consuming to establish, but they are less desirable than preventive controls because they usually occur in the reactive stage of the fraud cycle.

The ACFE (2016) found that the primary internal control weaknesses that allowed crimes to be committed in order of frequency were: lack of internal controls system; inadequate system; lack of management oversight and review; lack of independent audits; and lack of fraud education. Understanding how fraud exists helps auditors discover which internal controls must be established.

OPPORTUNITIES LEADING TO FRAUD

Out of all sides of the classic fraud triangle, opportunity is the one component that firms have the most influence over (Johnson & Rudolph, 2008). Opportunities to commit fraud can generally be closed through a strong and effectively maintained internal controls system.

Opportunities generally increase when an individual's position or authority is higher or when they are perceived to be more trustworthy than others (Laufer, 2011). This opportunity follows the fraud component of capability, where fraud perpetrators are often model employees (Gagliardi, 2014). Specific characteristics of small businesses, such as the organizational culture and climate, can also compound the opportunities available to potential fraud perpetrators (Murphy & Dacin, 2011).

NO INTERNAL CONTROLS SYSTEM

A lot of small businesses do not have any internal controls system. In fact, 29.3% of all businesses lack internal controls systems, and the percentage of small businesses that lack internal controls systems is even smaller (ACFE, 2016).

The main concern for many small businesses is that they lack the resources to set up an internal controls system (Laufer, 2011; Grollman & Colby, 1978; Schwartz, 2006). Larger organizations tend to spend more resources on preventing fraud—generally 2% of revenue for a $25 million revenue company (Schwartz, 2006). They are also able to maintain tip hotlines and provide extensive fraud training for employees (Laufer, 2011). This is especially important since 39% of fraud cases are discovered through tips, making it the most common detection method (ACFE, 2016). Organizations with hotlines are also more likely to detect fraud (ACFE, 2016). This puts small businesses at a disadvantage.

The resource constraint concern is reasonable, because some internal controls are time consuming to follow and others are expensive (such as surveillance technology). Grollman and Colby (1978) write that the cost of a perfect internal controls system can outweigh the potential benefits. Not all internal controls systems need to be expensive though. It is important to balance the costs versus the benefits of each internal control below before they are implemented (Schwartz, 2006).

WEAK HIRING PROCEDURES

Most business owners do not believe that their employees would even commit fraud (Gagliardi, 2014). However, research shows that 42% of the cases of occupational fraud are committed by employees or non-owners and are usually detected through tips (ACFE, 2016; Gagliardi, 2014). This is why internal controls that specifically target hiring procedures are so incredibly important. Even strong internal controls such as requiring background checks and reference checks before hiring prove inadequate, because employees who commit fraud are generally model employees who are willing to come in early and stay late (Gagliardi, 2014).

The efficacy of these controls is further in question, because 88.8% of fraud perpetrators have never been charged or convicted and 84% of perpetrators have never been punished or terminated (ACFE, 2016; Gagliardi, 2014). These statistics fall in line with the profile of most fraud perpetrators being common fraudsters as opposed to predators. The ACFE (2016) found that only 11% of background checks uncovered red flags that affected hiring decisions.

To help combat this weakness, small businesses can require rotation of duties or mandatory vacations (Johnson & Rudesill, 2001). This helps owners detect fraud once perpetrators are no longer on premise and able to conceal evidence of their fraud.

STAFFING CONSTRAINTS

The limited staff size is another characteristic that affects the risk of fraud within small businesses. Many fraud cases occur due to a lack of segregation of duties and management oversight (Carland et al., 2001; Laufer, 2011; Rea, 1981; Kapp & Heslop, 2011; Grollman, 1978; Gramling et al., 2010a). Staffing constraints affect the segregation of duties within a small business, because employees tend to wear more hats within small organizations (Kapp & Heslop, 2011; Gramling et al., 2010a). In fact, as Wells (2003) points out: most small businesses have "one-person accounting departments." This is especially a problem, because according to the ACFE (2016), the most common origin of fraud is from the accounting department.

This means the person who's opening the mail to collect checks and the person who's depositing the checks as well as recording them is often the same person. This leaves a huge opportunity for an employee to exploit this weakness. Trusting a single employee with more than one accounting activity provides opportunities to commit fraud (Johnson & Rudesill, 2001). It also forces small businesses to rely more on detective controls than preventive controls, because preventive controls usually require more staffing (Kapp & Heslop, 2011). An example of this is the detective internal control of requiring mandatory vacations, which can reveal fraud but requires employee coverage (Johnson & Rudolph, 2008).

PRESSURES AND RATIONALIZATION LEADING TO FRAUD

It can be quite difficult for businesses to counter the pressures that lead an individual to commit fraud. As broken down in modern fraud theory by both Lister (2007) and Murdock (2008) as analyzed above, the component of pressure can consist of financial, non-financial personal, employment or external, and social pressures. The motivation to commit fraud can stem from different areas of a perpetrator's life. However small businesses, can help mitigate some of the financial pressures by making sure to compensate employees well (Johnson & Rudolph, 2008).

By paying employees properly, small businesses can also minimize some of the rationalizations related to taking wages in kind that potential fraud perpetrators may enlist (Johnson & Rudolph, 2008). In addition, management that shows interest and tries to maintain a good work environment by treating employees well can help mitigate the rationalization behind fraud. These practices can help increase work morale and prevent resentments from occurring, which diminishes an individual's justification for fraud (Dennis, 2009).

Dennis (2009) recommends that employers remain sensitive to employee expectations in the hope of preventing resentment.

Other high-risk factors for fraud include low company loyalty and workforce motivation as these sentiments also provide rationalization opportunities (Finerman, 1995). Carland et al. (2001) identify associated risks such as being underpaid, underappreciated, general job dissatisfaction or the idea that the individual is only borrowing some money. Some of these risks ran be mitigated through careful hiring practices and employee screening (Johnson & Rudolph, 2008).

As can be seen, while the component of pressure is difficult to influence, employers can influence the rationalization component of fraud. Thus it is up to the small business owner or manager to be aware of fraud possibilities and prevent them from occurring. This is why many agree that management oversight is the most important factor in preventing fraud (Grollman, 1978; Leitch & Dillon, 1981; Johnson & Rudesill, 2001). They have the most impact on the maintenance of an internal controls system. This is because only 3% of fraudulent behavior is detected by external auditors—the majority are detected through insider tips (ACFE, 2016). Thus, small business owners are more engaged in the operations of their businesses and are more likely to detect suspicious activities than their bookkeepers or auditors. Since almost all frauds start small, internal controls that support fraud detection are just as important as those supporting fraud prevention (Johnson & Rudolph, 2008).

EMPLOYEE CAPABILITIES LEADING TO FRAUD

The possibility of being able to get away with fraud plays a large part in the psychology that motivates certain fraud perpetrators, "high capability" ones, to commit the crime. Even when detective controls do not discover any fraud, the adoption of internal controls can prevent individuals with high capability personalities from exploiting weaknesses (Murphy & Dacin, 2004). Knowing that they may get caught and punished is a strong deterrent (Carland et al., 2001; Rose et al., 2015; Kassem & Higson, 2012).

This perception of detection is shown previously in the slippery slope fraud model. Business owners can assess employees individually before hiring to combat this component. Similar to the recommendation of preventing rationalizations that lead to fraud, owners need to be more engaged in their businesses as well as providing more management oversight.

RECOMMENDED INTERNAL CONTROLS

As mentioned previously, the most vulnerable asset is cash. Thus, easy access to assets or accounting controls provides the opportunity for fraud to occur. This means that internal controls at the two main opportunity points of fraud related to cash, receipt and disbursement, are most important.

As noted above, cash receipts can be prone to skimming and larceny. Some internal control examples that address these two frequent asset misappropriation schemes were found through the literature review.

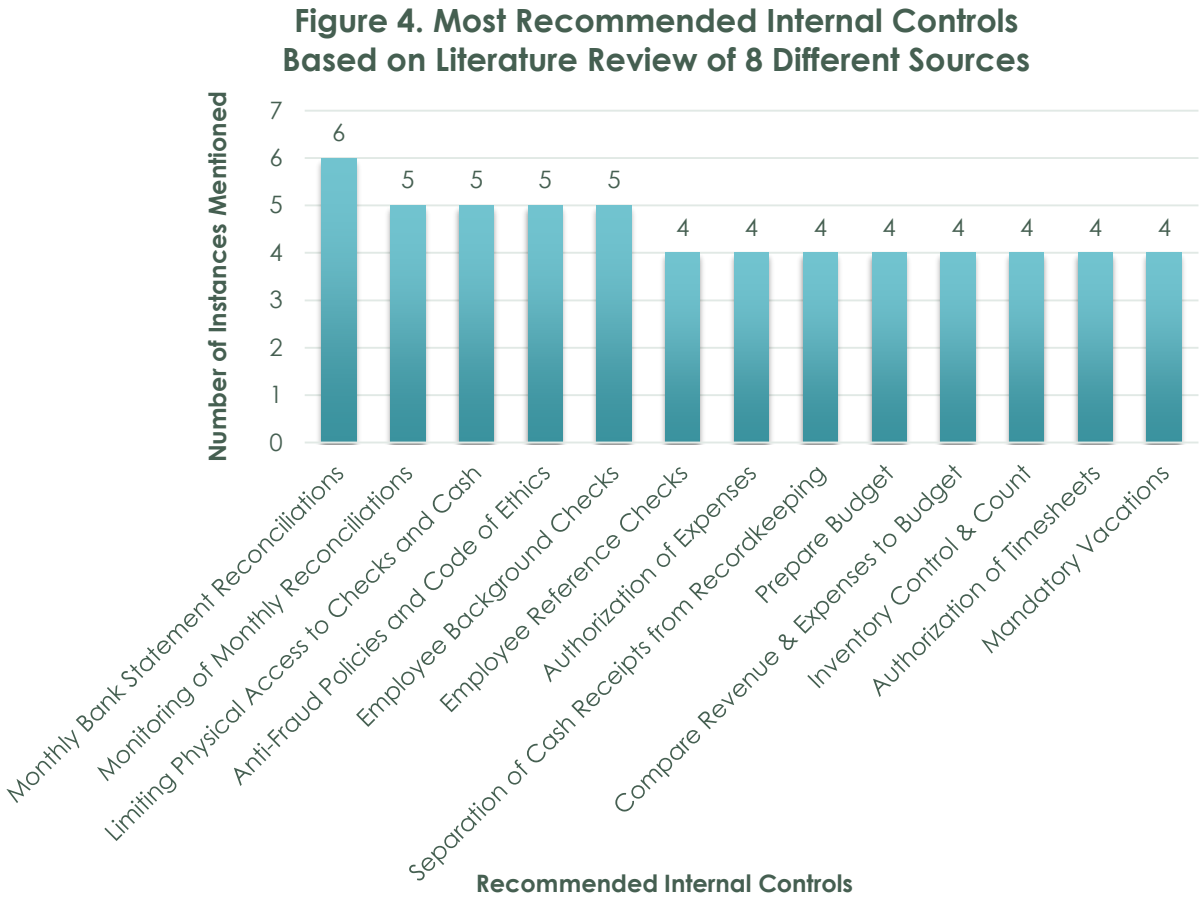
Controls for skimming schemes tend to be mainly preventive controls that require both resources from the company and time from management to implement. This is because skimming is an act that occurs off-book and does not involve any accounting records, which makes it a lot harder to discover through detective controls. Some examples for controls to prevent skimming are:

- Segregation of duties for cash receipts
- Lockbox usage
- Pre-numbering cash receipts
- Daily deposit/reconciliation of cash collections
- Cash refunds require managerial approval
- Video cameras
- Physical access controls

Controls for larceny schemes tend to be balanced between preventive and detective controls since larceny occurs on-book and after cash receipts have been recorded. Thus both preventive and detective controls work equally well to prevent these schemes. Some examples for controls that prevent and detect larceny are:

- Collect and deposit each day's receipts promptly
- Verify receivable transactions as legitimate
- Provide physical controls for cash and checks
- Verification of deposit slips versus accounting records by a third party
- Regular reconciliations and analysis of bank statements

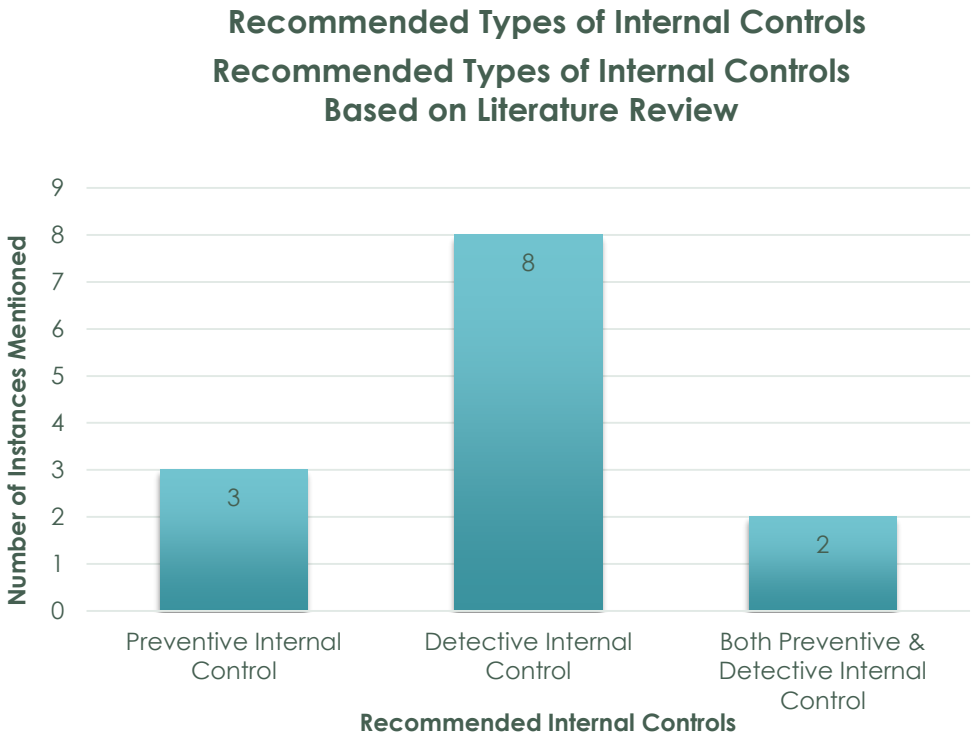
Figure 4 Most Recommended Internal Controls



Sources: Snyder et al., (1989); Small Business Fraud, (1997); Wells, (2003); Johnson & Rudolph, (2008); Gramling et al., (2010a); Kapp & Heslop, (2011); Laufer, (2011); ACFE, (2015).

There are also other general internal controls that should exist within every strong internal controls system. These are illustrated in Figure 4 and 5. Figure 4 illustrates the most recommended internal controls after reviewing eight sources that recommended specific internal controls. The recommended internal controls in Figure 4 overlap with some of the specific controls for skimming and larceny schemes. The biggest difference is that each of the controls in Figure 4 is also easily applicable to small businesses and start up businesses. The controls also balance costs and potential benefits.

Figure 5 Recommended Types of Internal Controls



Sources: Snyder et al., (1989); Small Business Fraud, (1997); Wells, (2003); Johnson & Rudolph, (2008); Gramling et al., (2010a); Kapp & Heslop, (2011); Laufer, (2011); ACFE, (2015).

Figure 5 shows how many of the most recommended internal controls from Figure 4 are either preventive or detective controls. This important because fraud prevention is usually much less expensive than fraud detection for a business (Laufer, 2011). The most accessible prevention controls for a small business are related to general controls; cash and asset controls; as well as payroll and hiring controls. They will be discussed further in the findings section.

Because of their staffing constraints, small businesses generally have to rely more heavily on detective controls (Kapp & Heslop, 2011). Because fraud starts small there's a need for detective controls to determine when fraud has occurred early on to prevent large losses (2008). As shown in the figure, there is a greater number of detective internal controls than preventive ones. This means that the recommended detective internal controls are better suited for a small business environment.

Some of the overarching internal controls that are recommended by researchers are mostly compensating controls. These overarching controls are managerial oversight, fraud training for employees, a clear non-tolerant anti-

fraud policy, and third party independent review (Gramling, 2010a; Johnson et al., 2014; Finerman, 1995; Leitch & Dillon, 1981).

Managerial oversight involves monthly reconciliations and keeping aware of what is occurring in the business through day to day involvement. A lot of this is simple awareness of whether or not sales are coming in, at what rate and what expenses are being charged. A basic understanding of fraud and awareness that fraud can occur in your business can go far (Gramling, 2010a). In addition, strong management can institute fraud training and a clear anti-fraud policy for employees; many third party organizations offer this as part of their business workshops (listed in Appendix A). Third party review is also essential and can be implemented through pro-bono CPAs, outside auditors or financial consultants.

Combined, these controls can offset any control deficiencies that exist within the internal controls system (Kapp & Heslop, 2011; Laufer, 2011). They act as "compensating" controls in that they address the opportunities, pressures, rationalization and capabilities that lead to occupational fraud.

EFFICACY OF INTERNAL CONTROLS

Though the efficacy of preventive controls can be difficult to measure, in the long run, preventive controls can save a business more money than detective ones (Laufer, 2011).

The 2009 Committee of Sponsoring Organizations (COSO) report on the Treadway Commission's Guidance on Monitoring Internal Controls System argues that simply establishing an internal controls system is not enough. The report suggests that internal controls systems require continual monitoring, otherwise they can be at risk of deteriorating over time. The report recommends monitoring through either a human manual monitor or through technology. Other researchers also agree with this view that a truly effective internal controls system requires consistency and continual monitoring (ACFE, 2016; Snyder et al.,1989; Schwartz, 2006; Ramamoorti & Dupree, 2010).

While the updated 2013 COSO report on the Guidance on Internal Control Integrated Framework echoes some of the concepts proposed by the 2009 report, it does underscore that a strong internal controls foundation is still the most reliable tool to address fraud. Thus, the final recommendation will require management oversight to include continual monitoring of the internal controls system to make sure that employees follow the internal controls established.

CLIENT RECOMMENDATIONS

CLIENT PROFILE

The client plans on opening a business selling plant-based foods and snacks that have a focus on ethical and sustainable sourcing. This would be the client's first business and the first time managing operations. As the client does not possess previous business experience and has described themselves as missing the 'math gene,' the client does not feel comfortable handling finance- or accounting-related decisions.

According to the business plan that was created for the client's business, the client will start off selling food at local farmers' markets until sales are high enough to support a crossover into selling the products in retail spaces. The client will only take cash or credit card through mobile payments. This money will immediately be deposited into a business checking account that is separated from the client's personal accounts. In the first year, the client will not hire any other employees, however starting the second year, they will most likely have to higher employees.

As business acumen is not the client's strong suite, this will provide a challenge to operating and sustaining the business without succumbing to fraud. Additional challenges include sourcing ingredients that align with the ethical and sustainable requirements at a price that would allow the business to still produce products that are priced to be able to sell. Altogether the main concerns regarding the business is that it is at high risk for fraud since management oversight would not be strong.

The goal is to provide the client with a comprehensive recommendation that acknowledges the unique challenges the business faces while taking into account the small size and start-up nature of the business.

INTERVIEW FINDINGS

This thesis not only utilizes a thorough literature review but also interviews with established professionals to develop a recommendation for best practices in internal controls for the client.

The first interview was with Lynn Kingston, a retired audit partner at Moss Adams, LLP in Portland, Oregon (Kingston, 2016). An audit professional and CPA since 1988, Kingston has provided professional services to a variety of clients. She has a wealth of experience working with small businesses. In addition, her unique

perspective as an auditor provided insights into which internal controls work for small size businesses and which are not as effective.

The second interview was with forensic investigator, Nancy Young (Young, 2016). Young is a certified public accountant, a certified fraud examiner, and a certified information systems auditor. Her three certifications have qualified her to perform extensive forensic audits, in coordination with the Portland Police Bureau, on cases of business fraud. Her ten years of first-hand experience working with small organization, provide insight into how devastating fraud can be to small businesses. The interview was very valuable in helping understand the underlying systems' weaknesses that leave small companies vulnerable to fraud.

The main recommendations gleaned from both interviews match the findings that the literature review provided. Kingston identified independence as the largest issue though and recommended that even if the client's business was less than 5 employees, there still should be an independent third party reviewer who would review the income and expenses monthly. This independent party would also review the monthly reconciliations provided by the bookkeeper.

The main reasoning behind this was that Kingston has encountered instances of bookkeeper fraud in small businesses before. She also recommended that once the business was a little larger, a mini-board be created to provide oversight in the running of the business. This mini-board could include a few board members that had understanding of financials to help with the management oversight aspect of an internal controls system. This could help make up some of the lack of business experience that the client has.

Young, in addition to recommendations similar to those of the literature review, also strongly recommended that the client go through workshops provided by not-for-profits and the U.S. Small Business Association. Workshops would help the client educate themselves on finance concepts and how accounting works. This education would help the client overcome their discomfort with numbers and would prevent the client from trusting employees or future business partners blindly. It would help inject an amount of skepticism, which Wells (2003) recommends business owners have as well. Workshops could also help the client understand how inventory tracking works helping minimize spoilage—a big concern in the food industry.

Young said that she sees new business owners encounter fraud quite often, since these owners are usually so focused on marketing and selling their products or services that they do not maintain the necessary focus on fraud prevention.

COMPREHENSIVE RECOMMENDATION

Given the findings from the literature review and interviews, the recommended internal controls for the client are as follows:

- Managerial oversight
- Fraud training for employees
- Clear non-tolerant anti-fraud policy
- Third party independent review

The managerial oversight control will be partly provided by the client and partly provided through a pro-bono lawyer or through the numerous business mentors that the client can sign up with. Multiple not-for-profits as well as government organizations provide small business mentorship programs that the client could take part in as listed in Appendix A. These resources are specifically geared towards small businesses or start ups and would therefore be well suited for the client's usage. It is strongly recommended that the client commits to attending business workshops, which are provided by the same organizations. Through these workshops, the client will be able to provide the fraud training and the clear non-tolerant anti-fraud policy themselves. The client also will be able to contribute their part in the management oversight that the business will require.

While a bookkeeper will maintain the necessary week to week accounting entries, the pro-bono lawyer or business mentor will review monthly bank reconciliations to identify any indicators of occupational fraud.

Thus in total, the following internal controls are recommended:

General Controls	• Monthly budget preparation (P) • Monthly comparisons of actual expenses to budget expenses (D) • Anti-fraud policies (P) • Authorization of business expenses by client (P) • Managerial oversight (P)
Cash and Asset Controls	• Lockboxes for cash (P) • Daily deposits of cash receipts (P) • Weekly inventory counts (D) • Monthly bank reconciliations (P/D) • Monthly monitoring of reconciliations (D)

Payroll and Hiring Controls	• Weekly review of employee timesheets (D) • Employee background checks (P) • Employee reference checks (P) • New employee fraud training (P)

These recommendations for internal controls also indicate which controls are preventive (P) and which are detective (D). In the client's case, there will be a pretty even mix of both. This way a comprehensive internal controls system can be established that addresses and prevents the opportunities, pressures, rationalization and capabilities that lead to occupational fraud.

CONCLUSION

Occupational fraud is growing for small businesses, as they are far more vulnerable to fraud than larger businesses. While the median loss per fraud case is the same, the frequency at which fraud occurs in smaller organizations is ten times the rate as in larger organizations (ACFE, 2016).

This is partly because small businesses possess unique characteristics that put them at a higher risk for fraud. Small businesses tend to have a culture that is too trusting of employees; they tend to lack adequate internal controls systems; and they have staffing constraints that affect the efficacy of internal controls even when they exist. In addition, when fraud occurs in small businesses, the effects are far more devastating. Studies show that the majority of small business failures can be attributed to occupational fraud (Carland et al., 2001).

To prevent fraud from occurring, an effective internal controls system must be established that utilizes both preventive and detective internal controls. This system will act as the foundation upon which business decisions will be made and transactions will be recorded. This internal controls system must also be continually monitored as these systems tend to deteriorate over time.

As part of the internal controls system; four main overarching internal controls are required to best address potential fraud in small businesses. They are:

1) managerial oversight;

2) anti-fraud policies;

3) anti-fraud training for employees; and

4) regular third party review of financials.

Together, these overarching internal controls, as well as the other controls recommended in this thesis, can help minimize asset misappropriation and help with the early detection of fraud to prevent losses before it's too late for a small business.

APPENDIX A: MENTOR & WORKSHOP RESOURCES

America's SBDC Oregon: CLIMB Center for Advancement
Getting Your Recipe to Market Program & Workshop
1626 SE Water Ave.
Portland, OR 97214
T: 971-722-5088
E: sbdc@pcc.com
https://www.pcc.edu/climb/small-business/launching/recipe.html
https://www.pcc.edu/climb/small-business/
http://www.bizcenter.org/

KitchenCru Business Workshops & Mentoring
337 NW Broadway St.
Portland, OR 97209
T: 503-223-1400
E: info@kitchencru.biz
http://www.kitchencru.biz/

MercyCorps Northwest Business Classes
43 SW Naito Parkway
Portland, OR 97204
T: 503-896-5070
https://www.mercycorpsnw.org

MicroMentors Northwest Business Mentoring
45 SW Ankeny St.
Portland, OR 97204
T: 503-465-4181
E: support@micromentor.org
https://www.micromentor.org

Oregon Entrepreneurs Network Business Resources
309 SW 6th Ave. Ste 212
Portland, OR 97204
T: 503.222.2270

https://www.oen.org

Port of Portland: Small Business Development
Minority, Women and Emerging Small Business Program (MWESB)
7200 NE Airport Way
Portland, OR 97218
T: 503-415-6587
E: kimberly.mitchell-phillips@portofportland.com
https://www2.portofportland.com/SmallBiz

Portland State University: Business Outreach Program
Small Business Workshops (Accounting Specific) and Mentoring
PO Box 751
Portland, OR 97207
T: 503-725-9820
E: psubop@pdx.edu
http://www.pdx.edu/business-outreach/

Portland State University: Impact Entrepreneurs
Small Business Workshops and Mentoring
PO Box 751
Portland, OR 97207
E: impactentrepreneurs@pdx.edu
http://www.pdx.edu/impactentrepreneurs/incubator

SCORE Business and Start Up Mentoring
620 SW Main St. Ste 313
Portland, OR 97205
https://portlandor.score.org/mentors

Starve Ups Start Up Mentoring
220 NW 8th Ave.
Portland, OR 97209
http://www.starveups.com

REFERENCES

Aguilar, M. K. (2010). Small Filers Struggle with Internal Controls over Fraud. *Compliance Week*. May, 33.

Albrecht, C. et al. (2015). The Role of Power in Financial Statement Fraud Schemes. *Journal of Business Ethics*. 131.4, 803–813.

Albrecht, C. et al. (2008). Current Trends in fraud and its detection. *Information Security Journal*. 17, 1-32.

Association of Certified Fraud Examiners (ACFE). (2015). *2015 U.S. Fraud Examiners Manual.* Austin: Association of Certified Fraud Examiners.

Association of Certified Fraud Examiners (ACFE). (2016). *Report to the Nations on Occupational Fraud and Abuse.* Austin: Association of Certified Fraud Examiners.

Camacho, L. (2009). A Review of 'Fraud Casebook: Lessons From the Bad Side of Business.' *Journal of Business and Finance Librarianship.* 14.4, 373–375.

Carland, J. W. et al. (2001). Fraud: A Concomitant Cause of Small Business Failure. *Entrepreneurial Executive*. 6, 73.

Christ, M. H. et al. (2015). Rotational Internal Audit Programs and Financial Reporting Quality: Do Compensating Controls Help?. *Accounting, Organizations and Society.* 44, 37–59.

Clark, C. S. (2011, October 27). Fraud Continues in Small Business Preference Programs. *Govexec.com*. n. page.

Cressey, D. R. (1953). "Other people's money; a study of the social psychology of embezzlement." Belmont: Wadsworth Publishing Company.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1987). Report of the National Commission on Fraudulent Financial Reporting. *Committee of Sponsoring Organizations of the Treadway Commission.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2009). Guidance on Monitoring Internal controls systems. *Committee of Sponsoring Organizations of the Treadway Commission.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control – Integrated Framework. *Committee of Sponsoring Organizations of the Treadway Commission.*

Daigle, R. J. et al. (2009). Small Businesses: Know Thy Enemy and Their methods. *The CPA Journal.* 2009, 30

Davis, J. S. & Pesch, H.L. (2012). Fraud Dynamics and Controls in Organizations. *Accounting, Organizations and Society.* 38.6-7, 469–483.

Dawson, S. (2015). *Internal Control/Anti-Fraud Program Design for the Small Business : A Guide for Companies Not Subject to the Sarbanes-Oxley Act.* Hoboken : Wiley Publishing.

Dennis, A. (2000). The Downside of Good Times. *Journal of Accountancy.* 190.5, 53.

Dodsworth, J. (1997). Putting Responsibility Where It Belongs: With the Client. *Accounting Today.* 1997, 19.

Dorminey, J. et al. (2012). The Evolution of Fraud Theory. *Issues in Accounting Education*. 27.2, 555-579.

Doost, R. K. (1990). Accounting irregularities and computer fraud. *The National Public Accountant*. May, 36-39.

Finerman, S. (1995). Understanding Fraud and Embezzlement. *Ohio CPA Journal.* 54.1, 37-40.

Fordham, D. R. (2012). Applying a Real-World Fraud to Multiple Learning Objectives: Considerations and an Example from the Systems Course. *Journal of Accounting Education.* 30.3-4, 325–354.

Gagliardi, C. (2014). The Reality of Fraud Risk: Five Common Misconceptions from Small Business Owners. *The CPA Journal*. 2014, 11.

Gordon, I. et al. (2012). Corporate Governance in Publicly Traded Small Firms: A Study of Canadian Venture Exchange Companies. *Business Horizons*. 55.6, 583–591.

Gramling, A. A. et al. (2010a). Addressing Problems with the Segregation of Duties in Smaller Companies. *The CPA Journal*. 2010, 30.

Gramling, A. A. et al. (2010b). Audit Partner Evaluation of Compensating Controls: A focus on design effectiveness and extent of auditor testing. *Auditing: A Journal of Practice and Theory.* 29-2, 175-187.

Audit Partner Evaluation of Compensating Controls: A focus on design effectiveness and extent of auditor testing. *Auditing: A Journal of Practice and Theory.* 29-2, 175-187.

Grollman, W. & Colby, R. (1978). Internal Control for Small Businesses: The Auditor of a Small Business Should Be Aware of Some Special Considerations. *Journal of Accountancy.* 146, 64–67.

Hodgetts, R.M. & Kuratko, D.F. (1998). *Effective Small Business Management.* 6th ed. Orlando: The Dryden Press.

Jackson, K. et al. (2010). Fraud Isn't Just For Big Business: Understanding the Drivers, Consequences, and Prevention of Fraud in Small Business. *Journal of International Management Studies*. 5.1, 160–164.

Johnson, G. G. & Rudesill, C.L. (2001). An Investigation into Fraud Prevention and Detection of Small Businesses in the United States: Responsibilities of Auditors, Managers, and Business Owners. *Accounting Forum.* 25.1, 56–78.

Johnson, L. R. & Rudolph, H.R. (2008). Prevent Large Cash Losses from Small Business Fraud. *Journal of Corporate Accounting and Finance*. 20.1, 37–44.

Johnson, S. et al. (2014). Mind Your Own Business: Bookkeeper Fraud in Small Business Organizations. *ProQuest Dissertations Publishing*. n. page.

Kapp, L. A. & Heslop, G. (2011). Protecting Small Businesses from Fraud: Simple Controls Can Reduce Opportunities. *The CPA Journal*. 2011, 62.

Kassem, R. & Higson, A. (2012). The New Fraud Triangle Model. *Journal of Emerging Trends in Economics and Management Sciences.* 3.3, 191-195.

Kingston, L. (2016). Interview regarding internal controls. Personal communication. May 5, 2016.

Laufer, D. (2011). Small Business Entrepreneurs: A Focus on Fraud Risk and prevention. *American Journal of Economics and Business Administration*. 3.2, 401–404.

Leitch, R. A. & Dillon, G.J. (1981). Internal Control Weaknesses in Small Businesses. *Journal of Accountancy*. 152.6, 97.

Lister, L. M. (2007). A practical approach to fraud risk. *Internal Auditor.* 2007, 1-30.

Mirshekary, S. & Carr, R. (2015). Effects of Exposure to Unethical Practices on the Personal Attitudes of Accountants in Small Accounting Firms. *Journal of Management and Organization.* 21.01, 98–106.

Murphy, P. & Dacin, T. (2011). Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations. *Journal of Business Ethics.* 101.4, 601–618.

Murdock, H. (2008). The three dimensions of fraud. *Internal Auditor*. 2008, 1-14.

Pressly, T. R. (2009). Combining Strategic Management and Internal Control Processes: A Recipe for Entrepreneurial Competitive Advantage. *Entrepreneurial Executive.* 14, 49.

Protect Small Business: Small Companies without Adequate Internal Controls Need CPAs to Help Them Minimize Fraud Risk. (2003). *Journal of Accountancy*. 195.3, 26–32.

Ramamoorti, S. & Dupree, J. (2010). Continuous Monitoring Can Help Deter and Prevent Fraud. *Financial Executives.* April, 66–67.

Rodgers, W. et al. (2015). Corporate Social Responsibility Enhanced Control Systems Reducing the Likelihood of Fraud. Journal of Business Ethics. 131.4, 871–882.

Rose, M. et al. (2015). A Boost to Fraud Risk Assessments. *Internal Auditor*. 2015, 22–23.

Schwartz, R. M. (2006). Make Risk Management and Internal Control Work for You: By Tailoring an Integrated, Business-Process-Based Template Solution, Small Companies Can Address Risks and Controls in a Cost-Effective Manner, Whether or Not SOX Compliance Is Mandated. *Strategic Finance.* 2006, 35.

Small Business, Big Losses: Audits and Hotlines Stack up as the Best Crime Busters in a New ACFE study. *Journal of Accountancy.* 198.6, 42–47.

Small Business Fraud. (1997). *Journal of Accountancy*. May, 1997.

Snyder, N. H. et al. (1989). Using Internal Controls to Reduce Employee Theft in Small Businesses. *Journal of Small Business Management*. 27.3, 48.

Taylor, N. (2002). Underreporting of Crime Against Small Businesses: Attitudes toward Police and Reporting Practices. *Journal of Business Ethics.* 13, 79–89.

U.S. Small Business Administration. (2016). Small Business Size Standards. *U.S. Small Business Administration.*

Vona, L. W. (2008). Fraud risk assessment: Building a fraud audit program. Hoboken: Wiley Publishing. 1-250.

Wells, J. T. (2007). *Fraud Casebook.* Hoboken: Wiley Publishing.

What You Don't Know Won't Hurt You: A Small Business Owner's Lack of Oversight Provides a Trusted Employee with Ample Opportunity to Steal from the company. (2011). *Internal Auditor.* 68.5, 71.

Wolfe, D. T. & Hermanson, D.R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*. 74.12, 38.

Young, N. (2016). Interview regarding internal controls and fraud prevention. Personal communication. May 19, 2016.